II

Calendar No. 181

112TH CONGRESS
1ST SESSION

S. 1151

To prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.

IN THE SENATE OF THE UNITED STATES

JUNE 7, 2011

Mr. LEAHY (for himself, Mr. SCHUMER, Mr. CARDIN, Mr. FRANKEN, and Mr. BLUMENTHAL) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

SEPTEMBER 22, 2011

Reported by Mr. LEAHY, with an amendment

[Strike out all after the enacting clause and insert the part printed in italic]

A BILL

To prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Personal Data Privacy and Security Act of 2011''.

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

SEC. 2. FINDINGS.

Congress finds that—

(1) databases of personally identifiable information are increasingly prime targets of hackers, identity thieves, rogue employees, and other criminals, including organized and sophisticated criminal operations;

(2) identity theft is a serious threat to the Nation's economic stability, homeland security, the development of e-commerce, and the privacy rights of Americans;

(3) over 9,300,000 individuals were victims of identity theft in America last year;

(4) security breaches are a serious threat to consumer confidence, homeland security, e-commerce, and economic stability;

(5) it is important for business entities that own, use, or license personally identifiable information to adopt reasonable procedures to ensure the security, privacy, and confidentiality of that personally identifiable information;

(6) individuals whose personal information has been compromised or who have been victims of identity theft should receive the necessary information and assistance to mitigate their damages and to restore the integrity of their personal information and identities;

(7) data brokers have assumed a significant role in providing identification, authentication, and screening services, and related data collection and analyses for commercial, nonprofit, and government operations;

(8) data misuse and use of inaccurate data have the potential to cause serious or irreparable harm to an individual's livelihood, privacy, and liberty and undermine efficient and effective business and government operations;

(9) there is a need to ensure that data brokers conduct their operations in a manner that prioritizes fairness, transparency, accuracy, and respect for the privacy of consumers;

(10) government access to commercial data can potentially improve safety, law enforcement, and national security; and

(11) because government use of commercial data containing personal information potentially af-

fects individual privacy, and law enforcement and national security operations, there is a need for Congress to exercise oversight over government use of commercial data.

SEC. 3. DEFINITIONS.

In this Act, the following definitions shall apply:

(1) AGENCY.—The term ''agency'' has the same meaning given such term in section 551 of title 5, United States Code.

(2) AFFILIATE.—The term ''affiliate'' means persons related by common ownership or by corporate control.

(3) BUSINESS ENTITY.—The term ''business entity'' means any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture established to make a profit, or nonprofit.

(4) IDENTITY THEFT.—The term ''identity theft'' means a violation of section 1028(a)(7) of title 18, United States Code.

(5) DATA BROKER.—The term ''data broker'' means a business entity which for monetary fees or dues regularly engages in the practice of collecting, transmitting, or providing access to sensitive personally identifiable information on more than 5,000 in-

dividuals who are not the customers or employees of that business entity or affiliate primarily for the purposes of providing such information to non-affiliated third parties on an interstate basis.

(6) DATA FURNISHER.—The term ''data furnisher'' means any agency, organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or nonprofit that serves as a source of information for a data broker.

(7) ENCRYPTION.—The term ''encryption''—

(A) means the protection of data in electronic form, in storage or in transit, using an encryption technology that has been adopted by a widely accepted standards setting body or, has been widely accepted as an effective industry practice which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data; and

(B) includes appropriate management and safeguards of such cryptographic keys so as to protect the integrity of the encryption.

(8) PERSONAL ELECTRONIC RECORD.—

(A) IN GENERAL.—The term ''personal electronic record'' means data associated with

an individual contained in a database, networked or integrated databases, or other data system that is provided by a data broker to nonaffiliated third parties and includes personally identifiable information about that individual.

(B) EXCLUSIONS.—The term ''personal electronic record'' does not include—

(i) any data related to an individual's past purchases of consumer goods; or

(ii) any proprietary assessment or evaluation of an individual or any proprietary assessment or evaluation of information about an individual.

(9) PERSONALLY IDENTIFIABLE INFORMATION.—The term ''personally identifiable information'' means any information, or compilation of information, in electronic or digital form that is a means of identification, as defined by section 1028(d)(7) of title 18, United State Code.

(10) PUBLIC RECORD SOURCE.—The term ''public record source'' means the Congress, any agency, any State or local government agency, the government of the District of Columbia and governments of the territories or possessions of the United

States, and Federal, State or local courts, courts martial and military commissions, that maintain personally identifiable information in records available to the public.

(11) SECURITY BREACH.—

(A) IN GENERAL.—The term ''security breach'' means compromise of the security, confidentiality, or integrity of computerized data through misrepresentation or actions—

(i) that result in, or that there is a reasonable basis to conclude has resulted in—

(I) the unauthorized acquisition of sensitive personally identifiable information; and

(II) access to sensitive personally identifiable information that is for an unauthorized purpose, or in excess of authorization; and

(ii) which present a significant risk of harm or fraud to any individual.

(B) EXCLUSION.—The term ''security breach'' does not include—

(i) a good faith acquisition of sensitive personally identifiable information by a

business entity or agency, or an employee or agent of a business entity or agency, if the sensitive personally identifiable information is not subject to further unauthorized disclosure;

(ii) the release of a public record not otherwise subject to confidentiality or nondisclosure requirements; or

(iii) any lawfully authorized investigative, protective, or intelligence activity of a law enforcement or intelligence agency of the United States.

(12) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.—The term ''sensitive personally identifiable information'' means any information or compilation of information, in electronic or digital form that includes—

(A) an individual's first and last name or first initial and last name in combination with any 1 of the following data elements:

(i) A non-truncated social security number, driver's license number, passport number, or alien registration number.

(ii) Any 2 of the following:

(I) Home address or telephone number.

(II) Mother's maiden name.

(III) Month, day, and year of birth.

(iii) Unique biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation.

(iv) A unique account identifier, electronic identification number, user name, or routing code in combination with any associated security code, access code, or password if the code or password is required for an individual to obtain money, goods, services, or any other thing of value; or

(B) a financial account number or credit or debit card number in combination with any security code, access code, or password that is required for an individual to obtain credit, withdraw funds, or engage in a financial transaction.

TITLE I—ENHANCING PUNISHMENT FOR IDENTITY THEFT AND OTHER VIOLATIONS OF DATA PRIVACY AND SECURITY

SEC. 101. ORGANIZED CRIMINAL ACTIVITY IN CONNECTION WITH UNAUTHORIZED ACCESS TO PERSONALLY IDENTIFIABLE INFORMATION.

Section 1961(1) of title 18, United States Code, is amended by inserting ''section 1030 (relating to fraud and related activity in connection with computers) if the act is a felony,'' before ''section 1084''.

SEC. 102. CONCEALMENT OF SECURITY BREACHES INVOLVING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by adding at the end the following:

''§ 1041. Concealment of security breaches involving sensitive personally identifiable information

''(a) Whoever, having knowledge of a security breach and having the obligation to provide notice of such breach to individuals under title III of the Personal Data Privacy and Security Act of 2011, and having not otherwise quali-

fied for an exemption from providing notice under section 312 of such Act, intentionally and willfully conceals the fact of such security breach and which breach causes economic damage to 1 or more persons, shall be fined under this title or imprisoned not more than 5 years, or both.

''(b) For purposes of subsection (a), the term 'person' has the same meaning as in section 1030(e)(12) of title 18, United States Code.

''(c) Any person seeking an exemption under section 312(b) of the Personal Data Privacy and Security Act of 2011 shall be immune from prosecution under this section if the United States Secret Service does not indicate, in writing, that such notice be given under section 312(b)(3) of such Act.''.

(b) CONFORMING AND TECHNICAL AMENDMENTS.—The table of sections for chapter 47 of title 18, United States Code, is amended by adding at the end the following:

''1041. Concealment of security breaches involving personally identifiable information.''.

(c) ENFORCEMENT AUTHORITY.—

(1) IN GENERAL.—The United States Secret Service shall have the authority to investigate offenses under this section.

(2) NONEXCLUSIVITY.—The authority granted in paragraph (1) shall not be exclusive of any existing authority held by any other Federal agency.

SEC. 103. PENALTIES FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030(c) of title 18, United States Code, is amended—

(1) by inserting ''or conspiracy'' after ''or an attempt'' each place it appears, except for paragraph (4);

(2) in paragraph (2)(B)—

(A) in clause (i), by inserting '', or attempt or conspiracy or conspiracy to commit an offense,'' after ''the offense'';

(B) in clause (ii), by inserting '', or attempt or conspiracy or conspiracy to commit an offense,'' after ''the offense''; and

(C) in clause (iii), by inserting ''(or, in the case of an attempted offense, would, if completed, have obtained)'' after ''information obtained''; and

(3) in paragraph (4)—

(A) in subparagraph (A)—

(i) by striking clause (ii);

(ii) by striking ''in the case of—'' and all that follows through ''an offense under subsection (a)(5)(B)'' and inserting ''in the case of an offense, or an attempt or conspiracy to commit an offense, under subsection (a)(5)(B)'';

(iii) by inserting ''or conspiracy'' after ''if the offense'';

(iv) by redesignating subclauses (I) through (VI) as clauses (i) through (vi), respectively, and adjusting the margin accordingly; and

(v) in clause (vi), as so redesignated, by striking ''; or'' and inserting a semicolon;

(B) in subparagraph (B)—

(i) by striking clause (ii);

(ii) by striking ''in the case of—'' and all that follows through ''an offense under subsection (a)(5)(A)'' and inserting ''in the case of an offense, or an attempt or conspiracy to commit an offense, under subsection (a)(5)(A)'';

(iii) by inserting ''or conspiracy'' after ''if the offense''; and

(iv) by striking ''; or'' and inserting a semicolon;

(C) in subparagraph (C)—

(i) by striking clause (ii);

(ii) by striking ''in the case of—'' and all that follows through ''an offense or an attempt to commit an offense'' and inserting ''in the case of an offense, or an attempt or conspiracy to commit an offense,''; and

(iii) by striking ''; or'' and inserting a semicolon;

(D) in subparagraph (D)—

(i) by striking clause (ii);

(ii) by striking ''in the case of—'' and all that follows through ''an offense or an attempt to commit an offense'' and inserting ''in the case of an offense, or an attempt or conspiracy to commit an offense,''; and

(iii) by striking ''; or'' and inserting a semicolon;

(E) in subparagraph (E), by inserting ''or conspires'' after ''offender attempts'';

(F) in subparagraph (F), by inserting ''or conspires'' after ''offender attempts''; and

(G) in subparagraph (G)(ii), by inserting ''or conspiracy'' after ''an attempt''.

TITLE II—DATA BROKERS

SEC. 201. TRANSPARENCY AND ACCURACY OF DATA COLLECTION.

(a) IN GENERAL.—Data brokers engaging in interstate commerce are subject to the requirements of this title for any product or service offered to third parties that allows access or use of personally identifiable information.

(b) LIMITATION.—Notwithstanding any other provision of this section, this section shall not apply to—

(1) any product or service offered by a data broker engaging in interstate commerce where such product or service is currently subject to, and in compliance with, access and accuracy protections similar to those under subsections (c) through (e) of this section under the Fair Credit Reporting Act (Public Law 91–508);

(2) any data broker that is subject to regulation under the Gramm-Leach-Bliley Act (Public Law 106–102);

(3) any data broker currently subject to and in compliance with the data security requirements for

such entities under the Health Insurance Portability and Accountability Act (Public Law 104–191), and its implementing regulations;

(4) any data broker subject to, and in compliance with, the privacy and data security requirements under sections 13401 and 13404 of division A of the American Reinvestment and Recovery Act of 2009 (42 U.S.C. 17931 and 17934) and implementing regulations promulgated under such sections;

(5) information in a personal electronic record that—

(A) the data broker has identified as inaccurate, but maintains for the purpose of aiding the data broker in preventing inaccurate information from entering an individual's personal electronic record; and

(B) is not maintained primarily for the purpose of transmitting or otherwise providing that information, or assessments based on that information, to nonaffiliated third parties;

(6) information concerning proprietary methodologies, techniques, scores, or algorithms relating to fraud prevention not normally provided to third parties in the ordinary course of business; and

~~(7) information that is used for legitimate governmental or fraud prevention purposes that would be compromised by disclosure to the individual.~~

~~(c) DISCLOSURES TO INDIVIDUALS.—~~

~~(1) IN GENERAL.—A data broker shall, upon the request of an individual, disclose to such individual for a reasonable fee all personal electronic records pertaining to that individual maintained or accessed by the data broker specifically for disclosure to third parties that request information on that individual in the ordinary course of business in the databases or systems of the data broker at the time of such request.~~

~~(2) INFORMATION ON HOW TO CORRECT INACCURACIES.—The disclosures required under paragraph (1) shall also include guidance to individuals on procedures for correcting inaccuracies.~~

~~(d) DISCLOSURE TO INDIVIDUALS OF ADVERSE ACTIONS TAKEN BY THIRD PARTIES.—~~

~~(1) IN GENERAL.—If a person takes any adverse action with respect to any individual that is based, in whole or in part, on any information contained in a personal electronic record, the person, at no cost to the affected individual, shall provide—~~

(A) written or electronic notice of the adverse action to the individual;

(B) to the individual, in writing or electronically, the name, address, and telephone number of the data broker (including a toll-free telephone number established by the data broker, if the data broker complies and maintains data on individuals on a nationwide basis) that furnished the information to the person;

(C) a copy of the information such person obtained from the data broker; and

(D) information to the individual on the procedures for correcting any inaccuracies in such information.

(2) ACCEPTED METHODS OF NOTICE.—A person shall be in compliance with the notice requirements under paragraph (1) if such person provides written or electronic notice in the same manner and using the same methods as are required under section 313(1) of this Act.

(c) ACCURACY RESOLUTION PROCESS.—

(1) INFORMATION FROM A PUBLIC RECORD OR LICENSOR.—

(A) IN GENERAL.—If an individual notifies a data broker of a dispute as to the complete-

ness or accuracy of information disclosed to such individual under subsection (c) that is obtained from a public record source or a license agreement, such data broker shall determine within 30 days whether the information in its system accurately and completely records the information available from the licensor or public record source.

(B) DATA BROKER ACTIONS.—If a data broker determines under subparagraph (A) that the information in its systems does not accurately and completely record the information available from a public record source or licensor, the data broker shall—

(i) correct any inaccuracies or incompleteness, and provide to such individual written notice of such changes; and

(ii) provide such individual with the contact information of the public record or licensor.

(2) INFORMATION NOT FROM A PUBLIC RECORD SOURCE OR LICENSOR.—If an individual notifies a data broker of a dispute as to the completeness or accuracy of information not from a public record or licensor that was disclosed to the individual under

subsection (c), the data broker shall, within 30 days of receiving notice of such dispute—

(A) review and consider free of charge any information submitted by such individual that is relevant to the completeness or accuracy of the disputed information; and

(B) correct any information found to be incomplete or inaccurate and provide notice to such individual of whether and what information was corrected, if any.

(3) EXTENSION OF REVIEW PERIOD.—The 30-day period described in paragraph (1) may be extended for not more than 30 additional days if a data broker receives information from the individual during the initial 30-day period that is relevant to the completeness or accuracy of any disputed information.

(4) NOTICE IDENTIFYING THE DATA FURNISHER.—If the completeness or accuracy of any information not from a public record source or licensor that was disclosed to an individual under subsection (c) is disputed by such individual, the data broker shall provide, upon the request of such individual, the contact information of any data furnisher that provided the disputed information.

(5) DETERMINATION THAT DISPUTE IS FRIVOLOUS OR IRRELEVANT.—

(A) IN GENERAL.—Notwithstanding paragraphs (1) through (3), a data broker may decline to investigate or terminate a review of information disputed by an individual under those paragraphs if the data broker reasonably determines that the dispute by the individual is frivolous or intended to perpetrate fraud.

(B) NOTICE.—A data broker shall notify an individual of a determination under subparagraph (A) within a reasonable time by any means available to such data broker.

SEC. 202. ENFORCEMENT.

(a) CIVIL PENALTIES.—

(1) PENALTIES.—Any data broker that violates the provisions of section 201 shall be subject to civil penalties of not more than $1,000 per violation per day while such violations persist, up to a maximum of $250,000 per violation.

(2) INTENTIONAL OR WILLFUL VIOLATION.—A data broker that intentionally or willfully violates the provisions of section 201 shall be subject to additional penalties in the amount of $1,000 per viola-

tion per day, to a maximum of an additional $250,000 per violation, while such violations persist.

(3) EQUITABLE RELIEF.—A data broker engaged in interstate commerce that violates this section may be enjoined from further violations by a court of competent jurisdiction.

(4) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this subsection are cumulative and shall not affect any other rights and remedies available under law.

(b) FEDERAL TRADE COMMISSION AUTHORITY.—Any data broker shall have the provisions of this title enforced against it by the Federal Trade Commission.

(c) STATE ENFORCEMENT.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State or any State or local law enforcement agency authorized by the State attorney general or by State statute to prosecute violations of consumer protection law, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the acts or practices of a data broker that violate this title, the State may bring a civil action on behalf of the residents of that State in a district court of the United

States of appropriate jurisdiction, or any other court of competent jurisdiction, to—

(A) enjoin that act or practice;

(B) enforce compliance with this title; or

(C) obtain civil penalties of not more than $1,000 per violation per day while such violations persist, up to a maximum of $250,000 per violation.

(2) NOTICE.—

(A) IN GENERAL.—Before filing an action under this subsection, the attorney general of the State involved shall provide to the Federal Trade Commission—

(i) a written notice of that action; and

(ii) a copy of the complaint for that action.

(B) EXCEPTION.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the attorney general of a State determines that it is not feasible to provide the notice described in subparagraph (A) before the filing of the action.

(C) NOTIFICATION WHEN PRACTICABLE.—In an action described under subparagraph (B),

the attorney general of a State shall provide the written notice and the copy of the complaint to the Federal Trade Commission as soon after the filing of the complaint as practicable.

(3) FEDERAL TRADE COMMISSION AUTHORITY.—Upon receiving notice under paragraph (2), the Federal Trade Commission shall have the right to—

(A) move to stay the action, pending the final disposition of a pending Federal proceeding or action as described in paragraph (4);

(B) intervene in an action brought under paragraph (1); and

(C) file petitions for appeal.

(4) PENDING PROCEEDINGS.—If the Federal Trade Commission has instituted a proceeding or civil action for a violation of this title, no attorney general of a State may, during the pendency of such proceeding or civil action, bring an action under this subsection against any defendant named in such civil action for any violation that is alleged in that civil action.

(5) RULE OF CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this title shall be construed to prevent an at-

torney general of a State from exercising the powers conferred on the attorney general by the laws of that State to—

(A) conduct investigations;

(B) administer oaths and affirmations; or

(C) compel the attendance of witnesses or the production of documentary and other evidence.

(6) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under this subsection may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

(B) SERVICE OF PROCESS.—In an action brought under this subsection, process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) may be found.

(d) NO PRIVATE CAUSE OF ACTION.—Nothing in this title establishes a private cause of action against a data broker for violation of any provision of this title.

SEC. 203. RELATION TO STATE LAWS.

No requirement or prohibition may be imposed under the laws of any State with respect to any subject matter

regulated under section 201, relating to individual access to, and correction of, personal electronic records held by data brokers.

SEC. 204. EFFECTIVE DATE.

This title shall take effect 180 days after the date of enactment of this Act.

TITLE III—PRIVACY AND SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION

Subtitle A—A Data Privacy and Security Program

SEC. 301. PURPOSE AND APPLICABILITY OF DATA PRIVACY AND SECURITY PROGRAM.

(a) PURPOSE.—The purpose of this subtitle is to ensure standards for developing and implementing administrative, technical, and physical safeguards to protect the security of sensitive personally identifiable information.

(b) IN GENERAL.—A business entity engaging in interstate commerce that involves collecting, accessing, transmitting, using, storing, or disposing of sensitive personally identifiable information in electronic or digital form on 10,000 or more United States persons is subject to the requirements for a data privacy and security program under section 302 for protecting sensitive personally identifiable information.

(c) LIMITATIONS.—Notwithstanding any other obligation under this subtitle, this subtitle does not apply to:

(1) FINANCIAL INSTITUTIONS.—Financial institutions—

(A) subject to the data security requirements and implementing regulations under the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.); and

(B) subject to—

(i) examinations for compliance with the requirements of this Act by a Federal Functional Regulator or State Insurance Authority (as those terms are defined in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809)); or

(ii) compliance with part 314 of title 16, Code of Federal Regulations.

(2) HIPPA REGULATED ENTITIES.—

(A) COVERED ENTITIES.—Covered entities subject to the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et seq.), including the data security requirements and implementing regulations of that Act.

(B) BUSINESS ENTITIES.—A Business entity shall be deemed in compliance with this Act if the business entity—

(i) is acting as a business associate, as that term is defined under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et seq.) and is in compliance with the requirements imposed under that Act and implementing regulations promulgated under that Act; and

(ii) is subject to, and currently in compliance, with the privacy and data security requirements under sections 13401 and 13404 of division A of the American Reinvestment and Recovery Act of 2009 (42 U.S.C. 17931 and 17934) and implementing regulations promulgated under such sections.

(3) PUBLIC RECORDS.—Public records not otherwise subject to a confidentiality or nondisclosure requirement, or information obtained from a news report or periodical.

(d) SAFE HARBORS.—

(1) IN GENERAL.—A business entity shall be deemed in compliance with the privacy and security program requirements under section 302 if the business entity complies with or provides protection equal to industry standards or standards widely accepted as an effective industry practice, as identified by the Federal Trade Commission, that are applicable to the type of sensitive personally identifiable information involved in the ordinary course of business of such business entity.

(2) LIMITATION.—Nothing in this subsection shall be construed to permit, and nothing does permit, the Federal Trade Commission to issue regulations requiring, or according greater legal status to, the implementation of or application of a specific technology or technological specifications for meeting the requirements of this title.

SEC. 302. REQUIREMENTS FOR A PERSONAL DATA PRIVACY AND SECURITY PROGRAM.

(a) PERSONAL DATA PRIVACY AND SECURITY PROGRAM.—A business entity subject to this subtitle shall comply with the following safeguards and any other administrative, technical, or physical safeguards identified by the Federal Trade Commission in a rulemaking process pursuant to section 553 of title 5, United States Code,

for the protection of sensitive personally identifiable information.

(1) SCOPE.—A business entity shall implement a comprehensive personal data privacy and security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the business entity and the nature and scope of its activities.

(2) DESIGN.—The personal data privacy and security program shall be designed to—

(A) ensure the privacy, security, and confidentiality of sensitive personally identifying information;

(B) protect against any anticipated vulnerabilities to the privacy, security, or integrity of sensitive personally identifying information; and

(C) protect against unauthorized access to use of sensitive personally identifying information that could create a significant risk of harm or fraud to any individual.

(3) RISK ASSESSMENT.—A business entity shall—

(A) identify reasonably foreseeable internal and external vulnerabilities that could result in

~~unauthorized access, disclosure, use, or alteration of sensitive personally identifiable information or systems containing sensitive personally identifiable information;~~

~~(B) assess the likelihood of and potential damage from unauthorized access, disclosure, use, or alteration of sensitive personally identifiable information;~~

~~(C) assess the sufficiency of its policies, technologies, and safeguards in place to control and minimize risks from unauthorized access, disclosure, use, or alteration of sensitive personally identifiable information; and~~

~~(D) assess the vulnerability of sensitive personally identifiable information during destruction and disposal of such information, including through the disposal or retirement of hardware.~~

~~(4) RISK MANAGEMENT AND CONTROL.—Each business entity shall—~~

~~(A) design its personal data privacy and security program to control the risks identified under paragraph (3); and~~

~~(B) adopt measures commensurate with the sensitivity of the data as well as the size,~~

complexity, and scope of the activities of the business entity that—

(i) control access to systems and facilities containing sensitive personally identifiable information, including controls to authenticate and permit access only to authorized individuals;

(ii) detect, record, and preserve information relevant to actual and attempted fraudulent, unlawful, or unauthorized access, disclosure, use, or alteration of sensitive personally identifiable information, including by employees and other individuals otherwise authorized to have access;

(iii) protect sensitive personally identifiable information during use, transmission, storage, and disposal by encryption, redaction, or access controls that are widely accepted as an effective industry practice or industry standard, or other reasonable means (including as directed for disposal of records under section 628 of the Fair Credit Reporting Act (15 U.S.C. 1681w) and the implementing regulations of such Act as set forth in section

682 of title 16, Code of Federal Regulations);

(iv) ensure that sensitive personally identifiable information is properly destroyed and disposed of, including during the destruction of computers, diskettes, and other electronic media that contain sensitive personally identifiable information;

(v) trace access to records containing sensitive personally identifiable information so that the business entity can determine who accessed or acquired such sensitive personally identifiable information pertaining to specific individuals; and

(vi) ensure that no third party or customer of the business entity is authorized to access or acquire sensitive personally identifiable information without the business entity first performing sufficient due diligence to ascertain, with reasonable certainty, that such information is being sought for a valid legal purpose.

(b) TRAINING.—Each business entity subject to this subtitle shall take steps to ensure employee training and

supervision for implementation of the data security program of the business entity.

(c) VULNERABILITY TESTING.—

(1) IN GENERAL.—Each business entity subject to this subtitle shall take steps to ensure regular testing of key controls, systems, and procedures of the personal data privacy and security program to detect, prevent, and respond to attacks or intrusions, or other system failures.

(2) FREQUENCY.—The frequency and nature of the tests required under paragraph (1) shall be determined by the risk assessment of the business entity under subsection (a)(3).

(d) RELATIONSHIP TO SERVICE PROVIDERS.—In the event a business entity subject to this subtitle engages service providers not subject to this subtitle, such business entity shall—

(1) exercise appropriate due diligence in selecting those service providers for responsibilities related to sensitive personally identifiable information, and take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the security, privacy, and integrity of the sensitive personally identifiable information at issue; and

(2) require those service providers by contract to implement and maintain appropriate measures designed to meet the objectives and requirements governing entities subject to section 301, this section, and subtitle B.

(c) PERIODIC ASSESSMENT AND PERSONAL DATA PRIVACY AND SECURITY MODERNIZATION.—Each business entity subject to this subtitle shall on a regular basis monitor, evaluate, and adjust, as appropriate its data privacy and security program in light of any relevant changes in—

(1) technology;

(2) the sensitivity of personally identifiable information;

(3) internal or external threats to personally identifiable information; and

(4) the changing business arrangements of the business entity, such as—

(A) mergers and acquisitions;

(B) alliances and joint ventures;

(C) outsourcing arrangements;

(D) bankruptcy; and

(E) changes to sensitive personally identifiable information systems.

(f) IMPLEMENTATION TIMELINE.—Not later than 1 year after the date of enactment of this Act, a business entity subject to the provisions of this subtitle shall implement a data privacy and security program pursuant to this subtitle.

SEC. 303. ENFORCEMENT.

(a) CIVIL PENALTIES.—

(1) IN GENERAL.—Any business entity that violates the provisions of sections 301 or 302 shall be subject to civil penalties of not more than $5,000 per violation per day while such a violation exists, with a maximum of $500,000 per violation.

(2) INTENTIONAL OR WILLFUL VIOLATION.—A business entity that intentionally or willfully violates the provisions of sections 301 or 302 shall be subject to additional penalties in the amount of $5,000 per violation per day while such a violation exists, with a maximum of an additional $500,000 per violation.

(3) EQUITABLE RELIEF.—A business entity engaged in interstate commerce that violates this section may be enjoined from further violations by a court of competent jurisdiction.

(4) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this section are

cumulative and shall not affect any other rights and remedies available under law.

(b) FEDERAL TRADE COMMISSION AUTHORITY.—Any business entity shall have the provisions of this subtitle enforced against it by the Federal Trade Commission.

(c) STATE ENFORCEMENT.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State or any State or local law enforcement agency authorized by the State attorney general or by State statute to prosecute violations of consumer protection law, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the acts or practices of a business entity that violate this subtitle, the State may bring a civil action on behalf of the residents of that State in a district court of the United States of appropriate jurisdiction, or any other court of competent jurisdiction, to—

(A) enjoin that act or practice;

(B) enforce compliance with this subtitle; or

(C) obtain civil penalties of not more than $5,000 per violation per day while such violations persist, up to a maximum of $500,000 per violation.

(2) NOTICE.—

(A) IN GENERAL.—Before filing an action under this subsection, the attorney general of the State involved shall provide to the Federal Trade Commission—

(i) a written notice of that action; and

(ii) a copy of the complaint for that action.

(B) EXCEPTION.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the attorney general of a State determines that it is not feasible to provide the notice described in this subparagraph before the filing of the action.

(C) NOTIFICATION WHEN PRACTICABLE.—In an action described under subparagraph (B), the attorney general of a State shall provide the written notice and the copy of the complaint to the Federal Trade Commission as soon after the filing of the complaint as practicable.

(3) FEDERAL TRADE COMMISSION AUTHORITY.—Upon receiving notice under paragraph (2), the Federal Trade Commission shall have the right to—

(A) move to stay the action, pending the final disposition of a pending Federal proceeding or action as described in paragraph (4);

(B) intervene in an action brought under paragraph (1); and

(C) file petitions for appeal.

(4) PENDING PROCEEDINGS.—If the Federal Trade Commission has instituted a proceeding or action for a violation of this subtitle or any regulations thereunder, no attorney general of a State may, during the pendency of such proceeding or action, bring an action under this subsection against any defendant named in such criminal proceeding or civil action for any violation that is alleged in that proceeding or action.

(5) RULE OF CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1) nothing in this subtitle shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to—

(A) conduct investigations;

(B) administer oaths and affirmations; or

(C) compel the attendance of witnesses or the production of documentary and other evidence.

(6) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under this subsection may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

(B) SERVICE OF PROCESS.—In an action brought under this subsection, process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) may be found.

(d) NO PRIVATE CAUSE OF ACTION.—Nothing in this subtitle establishes a private cause of action against a business entity for violation of any provision of this subtitle.

SEC. 304. RELATION TO OTHER LAWS.

(a) IN GENERAL.—No State may require any business entity subject to this subtitle to comply with any requirements with respect to administrative, technical, and physical safeguards for the protection of sensitive personally identifying information.

(b) LIMITATIONS.—Nothing in this subtitle shall be construed to modify, limit, or supersede the operation of the Gramm-Leach-Bliley Act or its implementing regulations, including those adopted or enforced by States.

Subtitle B—Security Breach Notification

SEC. 311. NOTICE TO INDIVIDUALS.

(a) IN GENERAL.—Any agency, or business entity engaged in interstate commerce, that uses, accesses, transmits, stores, disposes of or collects sensitive personally identifiable information shall, following the discovery of a security breach of such information, notify any resident of the United States whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed, or acquired.

(b) OBLIGATION OF OWNER OR LICENSEE.—

(1) NOTICE TO OWNER OR LICENSEE.—Any agency, or business entity engaged in interstate commerce, that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information that the agency or business entity does not own or license shall notify the owner or licensee of the information following the discovery of a security breach involving such information.

(2) NOTICE BY OWNER, LICENSEE OR OTHER DESIGNATED THIRD PARTY.—Nothing in this subtitle shall prevent or abrogate an agreement between an agency or business entity required to give notice under this section and a designated third party, including an owner or licensee of the sensitive personally identifiable information subject to the security breach, to provide the notifications required under subsection (a).

(3) BUSINESS ENTITY RELIEVED FROM GIVING NOTICE.—A business entity obligated to give notice under subsection (a) shall be relieved of such obligation if an owner or licensee of the sensitive personally identifiable information subject to the security breach, or other designated third party, provides such notification.

(c) TIMELINESS OF NOTIFICATION.—

(1) IN GENERAL.—All notifications required under this section shall be made without unreasonable delay following the discovery by the agency or business entity of a security breach.

(2) REASONABLE DELAY.—Reasonable delay under this subsection may include any time necessary to determine the scope of the security breach, prevent further disclosures, conduct the risk assess-

ment described in section 302(a)(3), and restore the reasonable integrity of the data system and provide notice to law enforcement when required.

(3) BURDEN OF PRODUCTION.—The agency, business entity, owner, or licensee required to provide notice under this subtitle shall, upon the request of the Attorney General, provide records or other evidence of the notifications required under this subtitle, including to the extent applicable, the reasons for any delay of notification.

(d) DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT PURPOSES.—

(1) IN GENERAL.—If a Federal law enforcement or intelligence agency determines that the notification required under this section would impede a criminal investigation, such notification shall be delayed upon written notice from such Federal law enforcement or intelligence agency to the agency or business entity that experienced the breach.

(2) EXTENDED DELAY OF NOTIFICATION.—If the notification required under subsection (a) is delayed pursuant to paragraph (1), an agency or business entity shall give notice 30 days after the day such law enforcement delay was invoked unless a Federal law enforcement or intelligence agency pro-

vides written notification that further delay is necessary.

(3) LAW ENFORCEMENT IMMUNITY.—No cause of action shall lie in any court against any law enforcement agency for acts relating to the delay of notification for law enforcement purposes under this subtitle.

SEC. 312. EXEMPTIONS.

(a) EXEMPTION FOR NATIONAL SECURITY AND LAW ENFORCEMENT.—

(1) IN GENERAL.—Section 311 shall not apply to an agency or business entity if the agency or business entity certifies, in writing, that notification of the security breach as required by section 311 reasonably could be expected to—

(A) cause damage to the national security; or

(B) hinder a law enforcement investigation or the ability of the agency to conduct law enforcement investigations.

(2) LIMITS ON CERTIFICATIONS.—An agency or business entity may not execute a certification under paragraph (1) to—

(A) conceal violations of law, inefficiency, or administrative error;

(B) prevent embarrassment to a business entity, organization, or agency; or

(C) restrain competition.

(3) NOTICE.—In every case in which an agency or business agency issues a certification under paragraph (1), the certification, accompanied by a description of the factual basis for the certification, shall be immediately provided to the United States Secret Service and the Federal Bureau of Investigation.

(4) SECRET SERVICE AND FBI REVIEW OF CERTIFICATIONS.—

(A) IN GENERAL.—The United States Secret Service or the Federal Bureau of Investigation may review a certification provided by an agency under paragraph (3), and shall review a certification provided by a business entity under paragraph (3), to determine whether an exemption under paragraph (1) is merited. Such review shall be completed not later than 10 business days after the date of receipt of the certification, except as provided in paragraph (5)(C).

(B) NOTICE.—Upon completing a review under subparagraph (A) the United States Secret Service or the Federal Bureau of Investiga-

tion shall immediately notify the agency or business entity, in writing, of its determination of whether an exemption under paragraph (1) is merited.

(C) EXEMPTION.—The exemption under paragraph (1) shall not apply if the United States Secret Service or the Federal Bureau of Investigation determines under this paragraph that the exemption is not merited.

(5) ADDITIONAL AUTHORITY OF THE SECRET SERVICE AND FBI.—

(A) IN GENERAL.—In determining under paragraph (4) whether an exemption under paragraph (1) is merited, the United States Secret Service or the Federal Bureau of Investigation may request additional information from the agency or business entity regarding the basis for the claimed exemption, if such additional information is necessary to determine whether the exemption is merited.

(B) REQUIRED COMPLIANCE.—Any agency or business entity that receives a request for additional information under subparagraph (A) shall cooperate with any such request.

(C) TIMING.—If the United States Secret Service or the Federal Bureau of Investigation requests additional information under subparagraph (A), the United States Secret Service or the Federal Bureau of Investigation shall notify the agency or business entity not later than 10 business days after the date of receipt of the additional information whether an exemption under paragraph (1) is merited.

(b) SAFE HARBOR.—An agency or business entity will be exempt from the notice requirements under section 311, if—

(1) a risk assessment concludes that—

(A) there is no significant risk that a security breach has resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach, with the encryption of such information establishing a presumption that no significant risk exists; or

(B) there is no significant risk that a security breach has resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach, with the rendering of such sen-

sitive personally identifiable information indecipherable through the use of best practices or methods, such as redaction, access controls, or other such mechanisms, which are widely accepted as an effective industry practice, or an effective industry standard, establishing a presumption that no significant risk exists;

(2) without unreasonable delay, but not later than 45 days after the discovery of a security breach, unless extended by the United States Secret Service or the Federal Bureau of Investigation, the agency or business entity notifies the United States Secret Service and the Federal Bureau of Investigation, in writing, of—

(A) the results of the risk assessment; and

(B) its decision to invoke the risk assessment exemption; and

(3) the United States Secret Service or the Federal Bureau of Investigation does not indicate, in writing, within 10 business days from receipt of the decision, that notice should be given.

(c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

(1) IN GENERAL.—A business entity will be exempt from the notice requirement under section 311

if the business entity utilizes or participates in a security program that—

(A) is designed to block the use of the sensitive personally identifiable information to initiate unauthorized financial transactions before they are charged to the account of the individual; and

(B) provides for notice to affected individuals after a security breach that has resulted in fraud or unauthorized transactions.

(2) LIMITATION.—The exemption by this subsection does not apply if—

(A) the information subject to the security breach includes sensitive personally identifiable information, other than a credit card or credit card security code, of any type of the sensitive personally identifiable information identified in section 3; or

(B) the security breach includes both the individual's credit card number and the individual's first and last name.

SEC. 313. METHODS OF NOTICE.

An agency or business entity shall be in compliance with section 311 if it provides both:

(1) INDIVIDUAL NOTICE.—Notice to individuals by 1 of the following means:

(A) Written notification to the last known home mailing address of the individual in the records of the agency or business entity.

(B) Telephone notice to the individual personally.

(C) E-mail notice, if the individual has consented to receive such notice and the notice is consistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001).

(2) MEDIA NOTICE.—Notice to major media outlets serving a State or jurisdiction, if the number of residents of such State whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person exceeds 5,000.

SEC. 314. CONTENT OF NOTIFICATION.

(a) IN GENERAL.—Regardless of the method by which notice is provided to individuals under section 313, such notice shall include, to the extent possible—

(1) a description of the categories of sensitive personally identifiable information that was, or is

reasonably believed to have been, accessed or acquired by an unauthorized person;

(2) a toll-free number—

(A) that the individual may use to contact the agency or business entity, or the agent of the agency or business entity; and

(B) from which the individual may learn what types of sensitive personally identifiable information the agency or business entity maintained about that individual; and

(3) the toll-free contact telephone numbers and addresses for the major credit reporting agencies.

(b) ADDITIONAL CONTENT.—Notwithstanding section 319, a State may require that a notice under subsection (a) shall also include information regarding victim protection assistance provided for by that State.

SEC. 315. COORDINATION OF NOTIFICATION WITH CREDIT REPORTING AGENCIES.

If an agency or business entity is required to provide notification to more than 5,000 individuals under section 311(a), the agency or business entity shall also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis (as defined in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)) of the timing and distribution of the no-

tices. Such notice shall be given to the consumer credit reporting agencies without unreasonable delay and, if it will not delay notice to the affected individuals, prior to the distribution of notices to the affected individuals.

SEC. 316. NOTICE TO LAW ENFORCEMENT.

(a) SECRET SERVICE AND FBI.—Any business entity or agency shall notify the United States Secret Service and the Federal Bureau of Investigation of the fact that a security breach has occurred if—

(1) the number of individuals whose sensitive personally identifying information was, or is reasonably believed to have been accessed or acquired by an unauthorized person exceeds 10,000;

(2) the security breach involves a database, networked or integrated databases, or other data system containing the sensitive personally identifiable information of more than 1,000,000 individuals nationwide;

(3) the security breach involves databases owned by the Federal Government; or

(4) the security breach involves primarily sensitive personally identifiable information of individuals known to the agency or business entity to be employees and contractors of the Federal Govern-

ment involved in national security or law enforcement.

(b) FTC REVIEW OF THRESHOLDS.—The Federal Trade Commission may review and adjust the thresholds for notice to law enforcement under subsection (a), after notice and the opportunity for public comment, in a manner consistent with this section.

(c) ADVANCE NOTICE TO LAW ENFORCEMENT.—Not later than 48 hours before notifying an individual of a security breach under section 311, a business entity or agency that is required to provide notice under this section shall notify the United States Secret Service and the Federal Bureau of Investigation of the fact that the business entity or agency intends to provide the notice.

(d) NOTICE TO OTHER LAW ENFORCEMENT AGENCIES.—The United States Secret Service and the Federal Bureau of Investigation shall be responsible for notifying—

(1) the United States Postal Inspection Service, if the security breach involves mail fraud;

(2) the attorney general of each State affected by the security breach; and

(3) the Federal Trade Commission, if the security breach involves consumer reporting agencies

subject to the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), or anticompetitive conduct.

(c) TIMING OF NOTICES.—The notices required under this section shall be delivered as follows:

(1) Notice under subsection (a) shall be delivered as promptly as possible, but not later than 14 days after discovery of the events requiring notice.

(2) Notice under subsection (d) shall be delivered not later than 14 days after the Service receives notice of a security breach from an agency or business entity.

SEC. 317. ENFORCEMENT.

(a) CIVIL ACTIONS BY THE ATTORNEY GENERAL.—The Attorney General may bring a civil action in the appropriate United States district court against any business entity that engages in conduct constituting a violation of this subtitle and, upon proof of such conduct by a preponderance of the evidence, such business entity shall be subject to a civil penalty of not more than $1,000 per day per individual whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, up to a maximum of $1,000,000 per violation, unless such conduct is found to be willful or intentional. In determining the amount of a civil penalty under this subsection, the court

shall take into account the degree of culpability of the business entity, any prior violations of this subtitle by the business entity, the ability of the business entity to pay, the effect on the ability of the business entity to continue to do business, and such other matters as justice may require.

(b) INJUNCTIVE ACTIONS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—If it appears that a business entity has engaged, or is engaged, in any act or practice constituting a violation of this subtitle, the Attorney General may petition an appropriate district court of the United States for an order—

(A) enjoining such act or practice; or

(B) enforcing compliance with this subtitle.

(2) ISSUANCE OF ORDER.—A court may issue an order under paragraph (1), if the court finds that the conduct in question constitutes a violation of this subtitle.

(c) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this subtitle are cumulative and shall not affect any other rights and remedies available under law.

(d) FRAUD ALERT.—Section 605A(b)(1) of the Fair Credit Reporting Act (15 U.S.C. 1681c–1(b)(1)) is

amended by inserting '', or evidence that the consumer has received notice that the consumer's financial information has or may have been compromised,'' after ''identity theft report''.

SEC. 318. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) IN GENERAL.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State or any State or local law enforcement agency authorized by the State attorney general or by State statute to prosecute violations of consumer protection law, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of a business entity in a practice that is prohibited under this subtitle, the State or the State or local law enforcement agency on behalf of the residents of the agency's jurisdiction, may bring a civil action on behalf of the residents of the State or jurisdiction in a district court of the United States of appropriate jurisdiction or any other court of competent jurisdiction, including a State court, to—

(A) enjoin that practice;

(B) enforce compliance with this subtitle; or

(C) civil penalties of not more than $1,000 per day per individual whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, up to a maximum of $1,000,000 per violation, unless such conduct is found to be willful or intentional.

(2) NOTICE.—

(A) IN GENERAL.—Before filing an action under paragraph (1), the attorney general of the State involved shall provide to the Attorney General of the United States—

(i) written notice of the action; and

(ii) a copy of the complaint for the action.

(B) EXEMPTION.—

(i) IN GENERAL.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subtitle, if the State attorney general determines that it is not feasible to provide the notice described in such subparagraph before the filing of the action.

(ii) NOTIFICATION.—In an action described in clause (i), the attorney general

of a State shall provide notice and a copy of the complaint to the Attorney General at the time the State attorney general files the action.

(b) FEDERAL PROCEEDINGS.—Upon receiving notice under subsection (a)(2), the Attorney General shall have the right to—

(1) move to stay the action, pending the final disposition of a pending Federal proceeding or action;

(2) initiate an action in the appropriate United States district court under section 317 and move to consolidate all pending actions, including State actions, in such court;

(3) intervene in an action brought under subsection (a)(2); and

(4) file petitions for appeal.

(c) PENDING PROCEEDINGS.—If the Attorney General has instituted a proceeding or action for a violation of this subtitle or any regulations thereunder, no attorney general of a State may, during the pendency of such proceeding or action, bring an action under this subtitle against any defendant named in such criminal proceeding or civil action for any violation that is alleged in that proceeding or action.

(d) CONSTRUCTION.—For purposes of bringing any civil action under subsection (a), nothing in this subtitle regarding notification shall be construed to prevent an attorney general of a State from exercising the powers conferred on such attorney general by the laws of that State to—

(1) conduct investigations;

(2) administer oaths or affirmations; or

(3) compel the attendance of witnesses or the production of documentary and other evidence.

(c) VENUE; SERVICE OF PROCESS.—

(1) VENUE.—Any action brought under subsection (a) may be brought in—

(A) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or

(B) another court of competent jurisdiction.

(2) SERVICE OF PROCESS.—In an action brought under subsection (a), process may be served in any district in which the defendant—

(A) is an inhabitant; or

(B) may be found.

(f) NO PRIVATE CAUSE OF ACTION.—Nothing in this subtitle establishes a private cause of action against a business entity for violation of any provision of this subtitle.

SEC. 319. EFFECT ON FEDERAL AND STATE LAW.

The provisions of this subtitle shall supersede any other provision of Federal law or any provision of law of any State relating to notification by a business entity engaged in interstate commerce or an agency of a security breach, except as provided in section 314(b).

SEC. 320. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated such sums as may be necessary to cover the costs incurred by the United States Secret Service to carry out investigations and risk assessments of security breaches as required under this subtitle.

SEC. 321. REPORTING ON RISK ASSESSMENT EXEMPTIONS.

The United States Secret Service and the Federal Bureau of Investigation shall report to Congress not later than 18 months after the date of enactment of this Act, and upon the request by Congress thereafter, on—

(1) the number and nature of the security breaches described in the notices filed by those business entities invoking the risk assessment exemption under section 312(b) and the response of the United

States Secret Service and the Federal Bureau of Investigation to such notices; and

(2) the number and nature of security breaches subject to the national security and law enforcement exemptions under section 312(a), provided that such report may not disclose the contents of any risk assessment provided to the United States Secret Service and the Federal Bureau of Investigation pursuant to this subtitle.

SEC. 322. EFFECTIVE DATE.

This subtitle shall take effect on the expiration of the date which is 90 days after the date of enactment of this Act.

TITLE IV—GOVERNMENT ACCESS TO AND USE OF COMMERCIAL DATA

SEC. 401. GENERAL SERVICES ADMINISTRATION REVIEW OF CONTRACTS.

(a) IN GENERAL.—In considering contract awards totaling more than $500,000 and entered into after the date of enactment of this Act with data brokers, the Administrator of the General Services Administration shall evaluate—

(1) the data privacy and security program of a data broker to ensure the privacy and security of

data containing personally identifiable information, including whether such program adequately addresses privacy and security threats created by malicious software or code, or the use of peer-to-peer file sharing software;

(2) the compliance of a data broker with such program;

(3) the extent to which the databases and systems containing personally identifiable information of a data broker have been compromised by security breaches; and

(4) the response by a data broker to such breaches, including the efforts by such data broker to mitigate the impact of such security breaches.

(b) COMPLIANCE SAFE HARBOR.—The data privacy and security program of a data broker shall be deemed sufficient for the purposes of subsection (a), if the data broker complies with or provides protection equal to industry standards, as identified by the Federal Trade Commission, that are applicable to the type of personally identifiable information involved in the ordinary course of business of such data broker.

(c) PENALTIES.—In awarding contracts with data brokers for products or services related to access, use, compilation, distribution, processing, analyzing, or evalu-

ating personally identifiable information, the Administrator of the General Services Administration shall—

(1) include monetary or other penalties—

(A) for failure to comply with subtitles A and B of title III; or

(B) if a contractor knows or has reason to know that the personally identifiable information being provided is inaccurate, and provides such inaccurate information; and

(2) require a data broker that engages service providers not subject to subtitle A of title III for responsibilities related to sensitive personally identifiable information to—

(A) exercise appropriate due diligence in selecting those service providers for responsibilities related to personally identifiable information;

(B) take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the security, privacy, and integrity of the personally identifiable information at issue; and

(C) require such service providers, by contract, to implement and maintain appropriate

measures designed to meet the objectives and requirements in title III.

(d) LIMITATION.—The penalties under subsection (c) shall not apply to a data broker providing information that is accurately and completely recorded from a public record source or licensor.

SEC. 402. REQUIREMENT TO AUDIT INFORMATION SECURITY PRACTICES OF CONTRACTORS AND THIRD PARTY BUSINESS ENTITIES.

Section 3544(b) of title 44, United States Code, is amended—

(1) in paragraph (7)(C)(iii), by striking ''and'' after the semicolon;

(2) in paragraph (8), by striking the period and inserting ''; and''; and

(3) by adding at the end the following:

''(9) procedures for evaluating and auditing the information security practices of contractors or third party business entities supporting the information systems or operations of the agency involving personally identifiable information (as that term is defined in section 3 of the Personal Data Privacy and Security Act of 2011) and ensuring remedial action to address any significant deficiencies.''.

SEC. 403. PRIVACY IMPACT ASSESSMENT OF GOVERNMENT USE OF COMMERCIAL INFORMATION SERVICES CONTAINING PERSONALLY IDENTIFIABLE INFORMATION.

(a) IN GENERAL.—Section 208(b)(1) of the E-Government Act of 2002 (44 U.S.C. 3501 note) is amended—

(1) in subparagraph (A)(i), by striking ''or''; and

(2) in subparagraph (A)(ii), by striking the period and inserting ''; or''; and

(3) by inserting after clause (ii) the following:

''(iii) purchasing or subscribing for a fee to personally identifiable information from a data broker (as such terms are defined in section 3 of the Personal Data Privacy and Security Act of 2011).''.

(b) LIMITATION.—Notwithstanding any other provision of law, commencing 1 year after the date of enactment of this Act, no Federal agency may enter into a contract with a data broker to access for a fee any database consisting primarily of personally identifiable information concerning United States persons (other than news reporting or telephone directories) unless the head of such department or agency—

(1) completes a privacy impact assessment under section 208 of the E-Government Act of 2002

~~(44 U.S.C. 3501 note), which shall subject to the provision in that Act pertaining to sensitive information, include a description of—~~

~~(A) such database;~~

~~(B) the name of the data broker from whom it is obtained; and~~

~~(C) the amount of the contract for use;~~

~~(2) adopts regulations that specify—~~

~~(A) the personnel permitted to access, analyze, or otherwise use such databases;~~

~~(B) standards governing the access, analysis, or use of such databases;~~

~~(C) any standards used to ensure that the personally identifiable information accessed, analyzed, or used is the minimum necessary to accomplish the intended legitimate purpose of the Federal agency;~~

~~(D) standards limiting the retention and redisclosure of personally identifiable information obtained from such databases;~~

~~(E) procedures ensuring that such data meet standards of accuracy, relevance, completeness, and timeliness;~~

(F) the auditing and security measures to protect against unauthorized access, analysis, use, or modification of data in such databases;

(G) applicable mechanisms by which individuals may secure timely redress for any adverse consequences wrongly incurred due to the access, analysis, or use of such databases;

(H) mechanisms, if any, for the enforcement and independent oversight of existing or planned procedures, policies, or guidelines; and

(I) an outline of enforcement mechanisms for accountability to protect individuals and the public against unlawful or illegitimate access or use of databases; and

(3) incorporates into the contract or other agreement totaling more than $500,000, provisions—

(A) providing for penalties—

(i) for failure to comply with title III of this Act; or

(ii) if the entity knows or has reason to know that the personally identifiable information being provided to the Federal department or agency is inaccurate, and provides such inaccurate information; and

(B) requiring a data broker that engages service providers not subject to subtitle A of title III for responsibilities related to sensitive personally identifiable information to—

(i) exercise appropriate due diligence in selecting those service providers for responsibilities related to personally identifiable information;

(ii) take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the security, privacy, and integrity of the personally identifiable information at issue; and

(iii) require such service providers, by contract, to implement and maintain appropriate measures designed to meet the objectives and requirements in title III.

(c) LIMITATION ON PENALTIES.—The penalties under subsection (b)(3)(A) shall not apply to a data broker providing information that is accurately and completely recorded from a public record source.

(d) STUDY OF GOVERNMENT USE.—

(1) SCOPE OF STUDY.—Not later than 180 days after the date of enactment of this Act, the

~~Comptroller General of the United States shall conduct a study and audit and prepare a report on Federal agency actions to address the recommendations in the Government Accountability Office's April 2006 report on agency adherence to key privacy principles in using data brokers or commercial databases containing personally identifiable information.~~

~~(2) REPORT.—A copy of the report required under paragraph (1) shall be submitted to Congress.~~

~~TITLE V—COMPLIANCE WITH STATUTORY PAY-AS-YOU-GO ACT~~

~~SEC. 501. BUDGET COMPLIANCE.~~

~~The budgetary effects of this Act, for the purpose of complying with the Statutory Pay-As-You-Go Act of 2010, shall be determined by reference to the latest statement titled "Budgetary Effects of PAYGO Legislation" for this Act, submitted for printing in the Congressional Record by the Chairman of the Senate Budget Committee, provided that such statement has been submitted prior to the vote on passage.~~

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Personal Data Privacy and Security Act of 2011".

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

SEC. 2. FINDINGS.

Congress finds that—

(1) databases of personally identifiable information are increasingly prime targets of hackers, iden-

tity thieves, rogue employees, and other criminals, including organized and sophisticated criminal operations;

(2) identity theft is a serious threat to the Nation's economic stability, national security, homeland security, cybersecurity, the development of e-commerce, and the privacy rights of Americans;

(3) security breaches are a serious threat to consumer confidence, homeland security, national security, e-commerce, and economic stability;

(4) it is important for business entities that own, use, or license personally identifiable information to adopt reasonable procedures to ensure the security, privacy, and confidentiality of that personally identifiable information;

(5) individuals whose personal information has been compromised or who have been victims of identity theft should receive the necessary information and assistance to mitigate their damages and to restore the integrity of their personal information and identities;

(6) data misuse and use of inaccurate data have the potential to cause serious or irreparable harm to an individual's livelihood, privacy, and liberty and

undermine efficient and effective business and government operations;

(7) government access to commercial data can potentially improve safety, law enforcement, and national security; and

(8) because government use of commercial data containing personal information potentially affects individual privacy, and law enforcement and national security operations, there is a need for Congress to exercise oversight over government use of commercial data.

SEC. 3. DEFINITIONS.

In this Act, the following definitions shall apply:

(1) AFFILIATE.—The term "affiliate" means persons related by common ownership or by corporate control.

(2) AGENCY.—The term "agency" has the same meaning given such term in section 551 of title 5, United States Code.

(3) BUSINESS ENTITY.—The term "business entity" means any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture established to make a profit, or nonprofit.

(4) DATA SYSTEM COMMUNICATION INFORMATION.—The term "data system communication information" means dialing, routing, addressing, or signaling information that identifies the origin, direction, destination, processing, transmission, or termination of each communication initiated, attempted, or received.

(5) DESIGNATED ENTITY.—The term "designated entity" means the Federal Government entity designated by the Secretary of Homeland Security under section 216(a).

(6) ENCRYPTION.—The term "encryption"—

(A) means the protection of data in electronic form, in storage or in transit, using an encryption technology that has been generally accepted by experts in the field of information security that renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data; and

(B) includes appropriate management and safeguards of such cryptographic keys so as to protect the integrity of the encryption.

(7) IDENTITY THEFT.—The term "identity theft" means a violation of section 1028(a)(7) of title 18, United States Code.

(8) PERSONALLY IDENTIFIABLE INFORMATION.—The term "personally identifiable information" means any information, or compilation of information, in electronic or digital form that is a means of identification, as defined by section 1028(d)(7) of title 18, United State Code.

(9) PUBLIC RECORD SOURCE.—The term "public record source" means the Congress, any agency, any State or local government agency, the government of the District of Columbia and governments of the territories or possessions of the United States, and Federal, State or local courts, courts martial and military commissions, that maintain personally identifiable information in records available to the public.

(10) SECURITY BREACH.—

(A) IN GENERAL.—The term "security breach" means compromise of the security, confidentiality, or integrity of, or the loss of, computerized data that result in, or that there is a reasonable basis to conclude has resulted in—

(i) the unauthorized acquisition of sensitive personally identifiable information; and

(ii) access to sensitive personally identifiable information that is for an unau-

thorized purpose, or in excess of authorization.

(B) EXCLUSION.—The term "security breach" does not include—

(i) a good faith acquisition of sensitive personally identifiable information by a business entity or agency, or an employee or agent of a business entity or agency, if the sensitive personally identifiable information is not subject to further unauthorized disclosure;

(ii) the release of a public record not otherwise subject to confidentiality or nondisclosure requirements or the release of information obtained from a public record, including information obtained from a news report or periodical; or

(iii) any lawfully authorized investigative, protective, or intelligence activity of a law enforcement or intelligence agency of the United States, a State, or a political subdivision of a State.

(11) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.—The term "sensitive personally identifiable information" means any information or com-

pilation of information, in electronic or digital form that includes the following:

(A) An individual's first and last name or first initial and last name in combination with any two of the following data elements:

(i) Home address or telephone number.

(ii) Mother's maiden name.

(iii) Month, day, and year of birth.

(B) A non-truncated social security number, driver's license number, passport number, or alien registration number or other government-issued unique identification number.

(C) Unique biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation.

(D) A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code.

(E) Any combination of the following data elements:

(i) An individual's first and last name or first initial and last name.

(ii) A unique account identifier, including a financial account number or cred-

it or debit card number, electronic identification number, user name, or routing code.

(iii) Any security code, access code, or password, or source code that could be used to generate such codes or passwords.

(12) SERVICE PROVIDER.—The term "service provider" means a business entity that provides electronic data transmission, routing, intermediate and transient storage, or connections to its system or network, where the business entity providing such services does not select or modify the content of the electronic data, is not the sender or the intended recipient of the data, and the business entity transmits, routes, stores, or provides connections for personal information in a manner that personal information is undifferentiated from other types of data that such business entity transmits, routes, stores, or provides connections. Any such business entity shall be treated as a service provider under this Act only to the extent that it is engaged in the provision of such transmission, routing, intermediate and transient storage or connections.

TITLE I—ENHANCING PUNISHMENT FOR IDENTITY THEFT AND OTHER VIOLATIONS OF DATA PRIVACY AND SECURITY

SEC. 101. ORGANIZED CRIMINAL ACTIVITY IN CONNECTION WITH UNAUTHORIZED ACCESS TO PERSONALLY IDENTIFIABLE INFORMATION.

Section 1961(1) of title 18, United States Code, is amended by inserting "section 1030 (relating to fraud and related activity in connection with computers) if the act is a felony," before "section 1084".

SEC. 102. CONCEALMENT OF SECURITY BREACHES INVOLVING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by adding at the end the following:

"§ 1041. Concealment of security breaches involving sensitive personally identifiable information

"(a) IN GENERAL.—Whoever, having knowledge of a security breach and of the fact that notice of such security breach is required under title II of the Personal Data Privacy and Security Act of 2011, intentionally and willfully conceals the fact of such security breach, shall, in the event that such security breach results in economic harm to any

individual in the amount of $1,000 or more, be fined under this tile or imprisoned for not more than 5 years, or both.

"(b) PERSON DEFINED.—For purposes of subsection (a), the term 'person' has the same meaning as in section 1030(e)(12) of title 18, United States Code.

"(c) NOTICE REQUIREMENT.—Any person seeking an exemption under section 212(b) of the Personal Data Privacy and Security Act of 2011 shall be immune from prosecution under this section if the Federal Trade Commission does not indicate, in writing, that such notice be given under section 212(b)(3) of such Act.".

(b) CONFORMING AND TECHNICAL AMENDMENTS.—The table of sections for chapter 47 of title 18, United States Code, is amended by adding at the end the following:

"1041. Concealment of security breaches involving sensitive personally identifiable information.".

(c) ENFORCEMENT AUTHORITY.—

(1) IN GENERAL.—The United States Secret Service and Federal Bureau of Investigation shall have the authority to investigate offenses under this section.

(2) NONEXCLUSIVITY.—The authority granted in paragraph (1) shall not be exclusive of any existing authority held by any other Federal agency.

SEC. 103. PENALTIES FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030(c) of title 18, United States Code, is amended to read as follows:

"(c) The punishment for an offense under subsection (a) or (b) of this section is—

"(1) a fine under this title or imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(1) of this section;

"(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than 3 years, or both, in the case of an offense under subsection (a)(2); or

"(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under paragraph (a)(2) of this section, if—

"(i) the offense was committed for purposes of commercial advantage or private financial gain;

"(ii) the offense was committee in the furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States, or of any State; or

"(iii) the value of the information obtained, or that would have been obtained if the offense was completed, exceeds $5,000;

"(3) a fine under this title or imprisonment for not more than 1 year, or both, in the case of an offense under subsection (a)(3) of this section;

"(4) a fine under this title or imprisonment of not more than 20 years, or both, in the case of an offense under subsection (a)(4) of this section;

"(5)(A) except as provided in subparagraph (D), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A) of this section, if the offense caused—

"(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

"(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

"(iii) physical injury to any person;

"(iv) a threat to public health or safety;

"(v) damage affecting a computer used by, or on behalf of, an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

"(vi) damage affecting 10 or more protected computers during any 1-year period;

"(B) a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(B), if the offense caused a harm provided in clause (i) through (vi) of subparagraph (A) of this subsection;

"(C) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both; or

"(D) a fine under this title, imprisonment for not more than 1 year, or both, for any other offense under subsection (a)(5);

"(6) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(6) of this section; or

"(7) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(7) of this section.".

SEC. 104. TRAFFICKING IN PASSWORDS.

Section 1030(a) of title 18, United States Code, is amended by striking paragraph (6) and inserting the following:

"(6) knowingly and with intent to defraud traffics (as defined in section 1029) in—

"(A) any password or similar information through which a protected computer as defined in subparagraphs (A) and (B) of subsection (e)(2) may be accessed without authorization; or

"(B) any means of access through which a protected computer as defined in subsection (e)(2)(A) may be accessed without authorization.".

SEC. 105. CONSPIRACY AND ATTEMPTED COMPUTER FRAUD OFFENSES.

Section 1030(b) of title 18, United States Code, is amended by inserting "for the completed offense" after "punished as provided".

SEC. 106. CRIMINAL AND CIVIL FORFEITURE FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030 of title 18, United States Code, is amended by striking subsections (i) and (j) and inserting the following:

"(i) CRIMINAL FORFEITURE.—

"(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

"(A) such person's interest in any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of such violation; and

"(B) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of such violation.

"(2) The criminal forfeiture of property under this subsection, including any seizure and disposition of the property, and any related judicial or administrative proceeding, shall be governed by the provisions

of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

"(j) CIVIL FORFEITURE.—

"(1) The following shall be subject to forfeiture to the United States and no property right, real or personal, shall exist in them:

"(A) Any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of any violation of this section, or a conspiracy to violate this section.

"(B) Any property, real or personal, constituting or derived from any gross proceeds obtained directly or indirectly, or any property traceable to such property, as a result of the commission of any violation of this section, or a conspiracy to violate this section.

"(2) Seizures and forfeitures under this subsection shall be governed by the provisions in chapter 46 of title 18, United States Code, relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) of title 18, United States Code, shall be performed by such officers, agents and other persons as may be designated for that purpose

by the Secretary of Homeland Security or the Attorney General.".

SEC. 107. LIMITATION ON CIVIL ACTIONS INVOLVING UNAUTHORIZED USE.

Section 1030(g) of title 18, United States Code, is amended—

(1) by inserting "(1)" before "Any person"; and

(2) by adding at the end the following:

"(2) No action may be brought under this subsection if a violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, constitutes the sole basis for determining that access to the protected computer is unauthorized, or in excess of authorization.".

SEC. 108. REPORTING OF CERTAIN CRIMINAL CASES.

Section 1030 of title 18, United States Code, is amended by adding at the end the following:

"(k) REPORTING CERTAIN CRIMINAL CASES.—Not later than 1 year after the date of the enactment of this Act, and annually thereafter, the Attorney General shall report to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives the number of criminal cases brought under subsection (a) that involve conduct in which —

"(1) the defendant—

"(A) exceeded authorized access to a non-governmental computer; or

"(B) accessed a non-governmental computer without authorization; and

"(2) the sole basis for the Government determining that access to the non-governmental computer was unauthorized, or in excess of authorization was that the defendant violated a contractual obligation or agreement with a service provider or employer, such as an acceptable use policy or terms of service agreement.".

SEC. 109. DAMAGE TO CRITICAL INFRASTRUCTURE COMPUTERS.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

"§ 1030A. Aggravated damage to a critical infrastructure computer

"(a) DEFINITIONS.—In this section—

"(1) the terms 'computer' and 'damage' have the meanings given such terms in section 1030; and

"(2) the term 'critical infrastructure computer' means a computer that manages or controls systems or assets vital to national defense, national security, national economic security, public health or safety, or

any combination of those matters, whether publicly or privately owned or operated, including—

"(A) gas and oil production, storage, and delivery systems;

"(B) water supply systems;

"(C) telecommunication networks;

"(D) electrical power delivery systems;

"(E) finance and banking systems;

"(F) emergency services;

"(G) transportation systems and services; and

"(H) government operations that provide essential services to the public

"(b) OFFENSE.—It shall be unlawful to, during and in relation to a felony violation of section 1030, intentionally cause or attempt to cause damage to a critical infrastructure computer, and such damage results in (or, in the case of an attempt, would, if completed have resulted in) the substantial impairment—

"(1) of the operation of the critical infrastructure computer; or

"(2) of the critical infrastructure associated with the computer.

"(c) PENALTY.—Any person who violates subsection (b) shall be fined under this title, imprisoned for not less than 3 years nor more than 20 years, or both.

"(d) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

"(1) a court shall not place on probation any person convicted of a violation of this section;

"(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment, including any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for the felony violation section 1030;

"(3) in determining any term of imprisonment to be imposed for a felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

"(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is

imposed by the court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.".

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

"1030A. Aggravated damage to a critical infrastructure computer.".

SEC. 110. LIMITATION ON ACTIONS INVOLVING UNAUTHORIZED USE.

Section 1030(e)(6) of title 18, United States Code, is amended by striking "alter;" and inserting "alter, but does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized;".

TITLE II—PRIVACY AND SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION

Subtitle A—A Data Privacy and Security Program

SEC. 201. PURPOSE AND APPLICABILITY OF DATA PRIVACY AND SECURITY PROGRAM.

(a) PURPOSE.—The purpose of this subtitle is to ensure standards for developing and implementing administrative, technical, and physical safeguards to protect the security of sensitive personally identifiable information.

(b) IN GENERAL.—A business entity engaging in interstate commerce that involves collecting, accessing, transmitting, using, storing, or disposing of sensitive personally identifiable information in electronic or digital form on 10,000 or more United States persons is subject to the requirements for a data privacy and security program under section 202 for protecting sensitive personally identifiable information.

(c) LIMITATIONS.—Notwithstanding any other obligation under this subtitle, this subtitle does not apply to the following:

(1) FINANCIAL INSTITUTIONS.—Financial institutions—

(A) subject to the data security requirements and standards under section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)); and

(B) subject to the jurisdiction of an agency or authority described in section 505(a) of the Gramm-Leach-Bliley Act (15 U.S.C. 6805(a)).

(2) HIPAA REGULATED ENTITIES.—

(A) COVERED ENTITIES.—Covered entities subject to the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et seq.), including the data security requirements and implementing regulations of that Act.

(B) BUSINESS ENTITIES.—A Business entity shall be deemed in compliance with this Act if the business entity—

(i) is acting as a business associate, as that term is defined under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et seq.) and is in compliance with the requirements imposed under that Act and implementing regulations promulgated under that Act; and

(ii) is subject to, and currently in compliance, with the privacy and data security

requirements under sections 13401 and 13404 of division A of the American Reinvestment and Recovery Act of 2009 (42 U.S.C. 17931 and 17934) and implementing regulations promulgated under such sections.

(3) SERVICE PROVIDERS.—A service provider for any electronic communication by a third-party, to the extent that the service provider is exclusively engaged in the transmission, routing, or temporary, intermediate, or transient storage of that communication.

(4) PUBLIC RECORDS.—Public records not otherwise subject to a confidentiality or nondisclosure requirement, or information obtained from a public record, including information obtained from a news report or periodical.

(d) SAFE HARBORS.—

(1) IN GENERAL.—A business entity shall be deemed in compliance with the privacy and security program requirements under section 202 if the business entity complies with or provides protection equal to industry standards or standards widely accepted as an effective industry practice, as identified by the Federal Trade Commission, that are applicable to the type of sensitive personally identifiable information

involved in the ordinary course of business of such business entity.

(2) LIMITATION.—Nothing in this subsection shall be construed to permit, and nothing does permit, the Federal Trade Commission to issue regulations requiring, or according greater legal status to, the implementation of or application of a specific technology or technological specifications for meeting the requirements of this title.

SEC. 202. REQUIREMENTS FOR A PERSONAL DATA PRIVACY AND SECURITY PROGRAM.

(a) PERSONAL DATA PRIVACY AND SECURITY PROGRAM.—A business entity subject to this subtitle shall comply with the following safeguards and any other administrative, technical, or physical safeguards identified by the Federal Trade Commission in a rulemaking process pursuant to section 553 of title 5, United States Code, for the protection of sensitive personally identifiable information:

(1) SCOPE.—A business entity shall implement a comprehensive personal data privacy and security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the business entity and the nature and scope of its activities.

(2) DESIGN.—The personal data privacy and security program shall be designed to—

(A) ensure the privacy, security, and confidentiality of sensitive personally identifying information;

(B) protect against any anticipated vulnerabilities to the privacy, security, or integrity of sensitive personally identifying information; and

(C) protect against unauthorized access to use of sensitive personally identifying information that could create a significant risk of harm or fraud to any individual.

(3) RISK ASSESSMENT.—A business entity shall—

(A) identify reasonably foreseeable internal and external vulnerabilities that could result in unauthorized access, disclosure, use, or alteration of sensitive personally identifiable information or systems containing sensitive personally identifiable information;

(B) assess the likelihood of and potential damage from unauthorized access, disclosure, use, or alteration of sensitive personally identifiable information;

(C) assess the sufficiency of its policies, technologies, and safeguards in place to control and minimize risks from unauthorized access, disclosure, use, or alteration of sensitive personally identifiable information; and

(D) assess the vulnerability of sensitive personally identifiable information during destruction and disposal of such information, including through the disposal or retirement of hardware.

(4) RISK MANAGEMENT AND CONTROL.—Each business entity shall—

(A) design its personal data privacy and security program to control the risks identified under paragraph (3);

(B) adopt measures commensurate with the sensitivity of the data as well as the size, complexity, and scope of the activities of the business entity that—

(i) control access to systems and facilities containing sensitive personally identifiable information, including controls to authenticate and permit access only to authorized individuals;

(ii) detect, record, and preserve information relevant to actual and attempted

fraudulent, unlawful, or unauthorized access, disclosure, use, or alteration of sensitive personally identifiable information, including by employees and other individuals otherwise authorized to have access;

(iii) protect sensitive personally identifiable information during use, transmission, storage, and disposal by encryption, redaction, or access controls that are widely accepted as an effective industry practice or industry standard, or other reasonable means (including as directed for disposal of records under section 628 of the Fair Credit Reporting Act (15 U.S.C. 1681w) and the implementing regulations of such Act as set forth in section 682 of title 16, Code of Federal Regulations);

(iv) ensure that sensitive personally identifiable information is properly destroyed and disposed of, including during the destruction of computers, diskettes, and other electronic media that contain sensitive personally identifiable information;

(v) trace access to records containing sensitive personally identifiable information

so that the business entity can determine who accessed or acquired such sensitive personally identifiable information pertaining to specific individuals; and

(vi) ensure that no third party or customer of the business entity is authorized to access or acquire sensitive personally identifiable information without the business entity first performing sufficient due diligence to ascertain, with reasonable certainty, that such information is being sought for a valid legal purpose; and

(C) establish a plan and procedures for minimizing the amount of sensitive personally identifiable information maintained by such business entity, which shall provide for the retention of sensitive personally identifiable information only as reasonably needed for the business purposes of such business entity or as necessary to comply with any legal obligation.

(b) TRAINING.—Each business entity subject to this subtitle shall take steps to ensure employee training and supervision for implementation of the data security program of the business entity.

(c) VULNERABILITY TESTING.—

(1) IN GENERAL.—Each business entity subject to this subtitle shall take steps to ensure regular testing of key controls, systems, and procedures of the personal data privacy and security program to detect, prevent, and respond to attacks or intrusions, or other system failures.

(2) FREQUENCY.—The frequency and nature of the tests required under paragraph (1) shall be determined by the risk assessment of the business entity under subsection (a)(3).

(d) RELATIONSHIP TO CERTAIN PROVIDERS OF SERVICES.—In the event a business entity subject to this subtitle engages a person or entity not subject to this subtitle (other than a service provider) to receive sensitive personally identifiable information in performing services or functions (other than the services or functions provided by a service provider) on behalf of and under the instruction of such business entity, such business entity shall—

(1) exercise appropriate due diligence in selecting the person or entity for responsibilities related to sensitive personally identifiable information, and take reasonable steps to select and retain a person or entity that is capable of maintaining appropriate safeguards for the security, privacy, and integrity of the

sensitive personally identifiable information at issue; and

(2) require the person or entity by contract to implement and maintain appropriate measures designed to meet the objectives and requirements governing entities subject to section 201, this section, and subtitle B.

(e) PERIODIC ASSESSMENT AND PERSONAL DATA PRIVACY AND SECURITY MODERNIZATION.—Each business entity subject to this subtitle shall on a regular basis monitor, evaluate, and adjust, as appropriate its data privacy and security program in light of any relevant changes in—

(1) technology;

(2) the sensitivity of personally identifiable information;

(3) internal or external threats to personally identifiable information; and

(4) the changing business arrangements of the business entity, such as—

(A) mergers and acquisitions;

(B) alliances and joint ventures;

(C) outsourcing arrangements;

(D) bankruptcy; and

(E) changes to sensitive personally identifiable information systems.

(f) IMPLEMENTATION TIMELINE.—Not later than 1 year after the date of enactment of this Act, a business entity subject to the provisions of this subtitle shall implement a data privacy and security program pursuant to this subtitle.

SEC. 203. ENFORCEMENT.

(a) CIVIL PENALTIES.—

(1) IN GENERAL.—Any business entity that violates the provisions of sections 201 or 202 shall be subject to civil penalties of not more than $5,000 per violation per day while such a violation exists, with a maximum of $500,000 per violation.

(2) INTENTIONAL OR WILLFUL VIOLATION.—A business entity that intentionally or willfully violates the provisions of sections 201 or 202 shall be subject to additional penalties in the amount of $5,000 per violation per day while such a violation exists, with a maximum of an additional $500,000 per violation.

(3) PENALTY LIMITS.—

(A) IN GENERAL.—Notwithstanding any other provision of law, the total sum of civil penalties assessed against a business entity for all violations of the provisions of this subtitle resulting from the same or related acts or omissions

shall not exceed $500,000, unless such conduct is found to be willful or intentional.

(B) DETERMINATIONS.—The determination of whether a violation of a provision of this subtitle has occurred, and if so, the amount of the penalty to be imposed, if any, shall be made by the court sitting as the finder of fact. The determination of whether a violation of a provision of this subtitle was willful or intentional, and if so, the amount of the additional penalty to be imposed, if any, shall be made by the court sitting as the finder of fact.

(C) ADDITIONAL PENALTY LIMIT.—If a court determines under subparagraph (B) that a violation of a provision of this subtitle was willful or intentional and imposes an additional penalty, the court may not impose an additional penalty in an amount that exceeds $500,000.

(4) EQUITABLE RELIEF.—A business entity engaged in interstate commerce that violates this section may be enjoined from further violations by a United States district court.

(5) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this section are cumu-

lative and shall not affect any other rights and remedies available under law.

(b) FEDERAL TRADE COMMISSION AUTHORITY.—Any business entity shall have the provisions of this subtitle enforced against it by the Federal Trade Commission.

(c) STATE ENFORCEMENT.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State or any State or local law enforcement agency authorized by the State attorney general or by State statute to prosecute violations of consumer protection law, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the acts or practices of a business entity that violate this subtitle, the State may bring a civil action on behalf of the residents of that State in a district court of the United States of appropriate jurisdiction to—

(A) enjoin that act or practice;

(B) enforce compliance with this subtitle; or

(C) obtain civil penalties of not more than $5,000 per violation per day while such violations persist, up to a maximum of $500,000 per violation.

(2) PENALTY LIMITS.—

(A) IN GENERAL.—Notwithstanding any other provision of law, the total sum of civil penalties assessed against a business entity for all violations of the provisions of this subtitle resulting from the same or related acts or omissions shall not exceed $500,000, unless such conduct is found to be willful or intentional.

(B) DETERMINATIONS.—The determination of whether a violation of a provision of this subtitle has occurred, and if so, the amount of the penalty to be imposed, if any, shall be made by the court sitting as the finder of fact. The determination of whether a violation of a provision of this subtitle was willful or intentional, and if so, the amount of the additional penalty to be imposed, if any, shall be made by the court sitting as the finder of fact.

(C) ADDITIONAL PENALTY LIMIT.—If a court determines under subparagraph (B) that a violation of a provision of this subtitle was willful or intentional and imposes an additional penalty, the court may not impose an additional penalty in an amount that exceeds $500,000.

(3) NOTICE.—

(A) IN GENERAL.—Before filing an action under this subsection, the attorney general of the State involved shall provide to the Federal Trade Commission—

(i) a written notice of that action; and

(ii) a copy of the complaint for that action.

(B) EXCEPTION.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the attorney general of a State determines that it is not feasible to provide the notice described in this subparagraph before the filing of the action.

(C) NOTIFICATION WHEN PRACTICABLE.—In an action described under subparagraph (B), the attorney general of a State shall provide the written notice and the copy of the complaint to the Federal Trade Commission as soon after the filing of the complaint as practicable.

(4) FEDERAL TRADE COMMISSION AUTHORITY.—Upon receiving notice under paragraph (2), the Federal Trade Commission shall have the right to—

(A) move to stay the action, pending the final disposition of a pending Federal proceeding or action as described in paragraph (4);

(B) intervene in an action brought under paragraph (1); and

(C) file petitions for appeal.

(5) PENDING PROCEEDINGS.—If the Federal Trade Commission initiates a Federal civil action for a violation of this subtitle, or any regulations thereunder, no attorney general of a State may bring an action for a violation of this subtitle that resulted from the same or related acts or omissions against a defendant named in the Federal civil action initiated by the Federal Trade Commission.

(6) RULE OF CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1) nothing in this subtitle shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to—

(A) conduct investigations;

(B) administer oaths and affirmations; or

(C) compel the attendance of witnesses or the production of documentary and other evidence.

(7) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under this subsection may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

(B) SERVICE OF PROCESS.—In an action brought under this subsection, process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) may be found.

(d) NO PRIVATE CAUSE OF ACTION.—Nothing in this subtitle establishes a private cause of action against a business entity for violation of any provision of this subtitle.

SEC. 204. RELATION TO OTHER LAWS.

(a) IN GENERAL.—No State may require any business entity subject to this subtitle to comply with any requirements with respect to administrative, technical, and physical safeguards for the protection of personal information.

(b) LIMITATIONS.—Nothing in this subtitle shall be construed to modify, limit, or supersede the operation of the Gramm-Leach-Bliley Act or its implementing regulations, including those adopted or enforced by States.

Subtitle B—Security Breach Notification

SEC. 211. NOTICE TO INDIVIDUALS.

(a) IN GENERAL.—Any agency, or business entity engaged in interstate commerce, other than a service provider, that uses, accesses, transmits, stores, disposes of or collects sensitive personally identifiable information shall, following the discovery of a security breach of such information, notify any resident of the United States whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed, or acquired.

(b) OBLIGATION OF OWNER OR LICENSEE.—

(1) NOTICE TO OWNER OR LICENSEE.—Any agency, or business entity engaged in interstate commerce, that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information that the agency or business entity does not own or license shall notify the owner or licensee of the information following the discovery of a security breach involving such information.

(2) NOTICE BY OWNER, LICENSEE, OR OTHER DESIGNATED THIRD PARTY.—Nothing in this subtitle shall prevent or abrogate an agreement between an agency or business entity required to give notice under this section and a designated third party, in-

cluding an owner or licensee of the sensitive personally identifiable information subject to the security breach, to provide the notifications required under subsection (a).

(3) BUSINESS ENTITY RELIEVED FROM GIVING NOTICE.—A business entity obligated to give notice under subsection (a) shall be relieved of such obligation if an owner or licensee of the sensitive personally identifiable information subject to the security breach, or other designated third party, provides such notification.

(4) SERVICE PROVIDERS.—If a service provider becomes aware of a security breach of data in electronic form containing sensitive personal information that is owned or possessed by another business entity that connects to or uses a system or network provided by the service provider for the purpose of transmitting, routing, or providing intermediate or transient storage of such data, the service provider shall be required to notify the business entity who initiated such connection, transmission, routing, or storage of the security breach if the business entity can be reasonably identified. Upon receiving such notification from a service provider, the business entity shall be required

to provide the notification required under subsection (a).

(c) TIMELINESS OF NOTIFICATION.—

(1) IN GENERAL.—All notifications required under this section shall be made without unreasonable delay following the discovery by the agency or business entity of a security breach.

(2) REASONABLE DELAY.—

(A) IN GENERAL.—Reasonable delay under this subsection may include any time necessary to determine the scope of the security breach, prevent further disclosures, conduct the risk assessment described in section 202(a)(3), and restore the reasonable integrity of the data system and provide notice to law enforcement when required.

(B) EXTENSION.—

(i) IN GENERAL.—Except as provided in section 212, delay of notification shall not exceed 60 days following the discovery of the security breach, unless the business entity or agency request an extension of time and the Federal Trade Commission determines in writing that additional time is reasonably necessary to determine the scope of the security breach, prevent further dis-

closures, conduct the risk assessment, restore the reasonable integrity of the data system, or to provide notice to the entity designated by the Secretary of Homeland Security pursuant to section 216.

(ii) APPROVAL OF REQUEST.—If the Federal Trade Commission approves the request for delay, the agency or business entity may delay the time period for notification for additional periods of up to 30 days.

(3) BURDEN OF PRODUCTION.—The agency, business entity, owner, or licensee required to provide notice under this subtitle shall, upon the request of the Attorney General or the Federal Trade Commission provide records or other evidence of the notifications required under this subtitle, including to the extent applicable, the reasons for any delay of notification.

(d) DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT OR NATIONAL SECURITY PURPOSES.—

(1) IN GENERAL.—If the United States Secret Service or the Federal Bureau of Investigation determines that the notification required under this section would impede a criminal investigation, or national security activity, such notification shall be delayed upon written notice from the United States Secret

Service or the Federal Bureau of Investigation to the agency or business entity that experienced the breach. The notification from the United States Secret Service or the Federal Bureau of Investigation shall specify in writing the period of delay requested for law enforcement or national security purposes.

(2) EXTENDED DELAY OF NOTIFICATION.—If the notification required under subsection (a) is delayed pursuant to paragraph (1), an agency or business entity shall give notice 30 days after the day such law enforcement or national security delay was invoked unless a Federal law enforcement or intelligence agency provides written notification that further delay is necessary.

(3) LAW ENFORCEMENT IMMUNITY.—No non-constitutional cause of action shall lie in any court against any agency for acts relating to the delay of notification for law enforcement or national security purposes under this subtitle.

(e) LIMITATIONS.—Notwithstanding any other obligation under this subtitle, this subtitle does not apply to the following:

(1) FINANCIAL INSTITUTIONS.—Financial institutions—

(A) subject to the data security requirements and standards under section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)); and

(B) subject to the jurisdiction of an agency or authority described in section 505(a) of the Gramm-Leach-Bliley Act (15 U.S.C. 6805(a)).

(2) HIPAA REGULATED ENTITIES.—

(A) COVERED ENTITIES.—Covered entities subject to the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et seq.), including the data security requirements and implementing regulations of that Act.

(B) BUSINESS ENTITIES.—A Business entity shall be deemed in compliance with this Act if the business entity—

(i)(I) is acting as a covered entity and as a business associate, as those terms are defined under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et seq.) and is in compliance with the requirements imposed under that Act and implementing regulations promulgated under that Act; and

(II) is subject to, and currently in compliance, with the data breach notification, privacy and data security requirements under the Health Information Technology for Economic and Clinical Health (HITECH) Act, (42 U.S.C. 17932) and implementing regulations promulgated thereunder; or

(ii) is acting as a vendor of personal health records and third party service provider, subject to the Health Information Technology for Economic and Clinical Health (HITECH) Act (42 U.S.C. 17937), including the data breach notification requirements and implementing regulations of that Act.

SEC. 212. EXEMPTIONS.

(a) EXEMPTION FOR NATIONAL SECURITY AND LAW ENFORCEMENT.—

(1) IN GENERAL.—Section 211 shall not apply to an agency or business entity if—

(A) the United States Secret Service or the Federal Bureau of Investigation determines that notification of the security breach could be expected to reveal sensitive sources and methods or

similarly impede the ability of the Government to conduct law enforcement investigations; or

(B) the Federal Bureau of Investigation determines that notification of the security breach could be expected to cause damage to the national security.

(2) IMMUNITY.—No non-constitutional cause of action shall lie in any court against any Federal agency for acts relating to the exemption from notification for law enforcement or national security purposes under this title.

(b) SAFE HARBOR.—

(1) IN GENERAL.—An agency or business entity shall be exempt from the notice requirements under section 211, if—

(A) a risk assessment conducted by the agency or business entity concludes that, based upon the information available, there is no significant risk that a security breach has resulted in, or will result in, identity theft, economic loss or harm, or physical harm to the individuals whose sensitive personally identifiable information was subject to the security breach;

(B) without unreasonable delay, but not later than 45 days after the discovery of a secu-

rity breach, unless extended by the Federal Trade Commission, the agency or business entity notifies the Federal Trade Commission, in writing, of—

(i) the results of the risk assessment; and

(ii) its decision to invoke the risk assessment exemption; and

(C) the Federal Trade Commission does not indicate, in writing, within 10 business days from receipt of the decision, that notice should be given.

(2) REBUTTABLE PRESUMPTIONS.—For purposes of paragraph (1)—

(A) the encryption of sensitive personally identifiable information described in paragraph (1)(A)(i) shall establish a rebuttable presumption that no significant risk exists; and

(B) the rendering of sensitive personally identifiable information described in paragraph (1)(A)(ii) unusable, unreadable, or indecipherable through data security technology or methodology that is generally accepted by experts in the field of information security, such as redaction

or access controls shall establish a rebuttable presumption that no significant risk exists.

(3) VIOLATION.—It shall be a violation of this section to—

(A) fail to conduct the risk assessment in a reasonable manner, or according to standards generally accepted by experts in the field of information security; or

(B) submit the results of a risk assessment that contains fraudulent or deliberately misleading information.

(c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

(1) IN GENERAL.—A business entity will be exempt from the notice requirement under section 211 if the business entity utilizes or participates in a security program that—

(A) effectively blocks the use of the sensitive personally identifiable information to initiate unauthorized financial transactions before they are charged to the account of the individual; and

(B) provides for notice to affected individuals after a security breach that has resulted in fraud or unauthorized transactions.

(2) LIMITATION.—The exemption in paragraph (1) does not apply if the information subject to the

security breach includes an individual's first and last name, or any other type of sensitive personally identifiable information as defined in section 3, unless that information is only a credit card number or credit card security code.

SEC. 213. METHODS OF NOTICE.

An agency or business entity shall be in compliance with section 211 if it provides the following:

(1) INDIVIDUAL NOTICE.—Notice to individuals by 1 of the following means:

(A) Written notification to the last known home mailing address of the individual in the records of the agency or business entity.

(B) Telephone notice to the individual personally.

(C) E-mail notice, if the individual has consented to receive such notice and the notice is consistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001).

(2) MEDIA NOTICE.—Notice to major media outlets serving a State or jurisdiction, if the number of residents of such State whose sensitive personally identifiable information was, or is reasonably believed

to have been, accessed or acquired by an unauthorized person exceeds 5,000.

SEC. 214. CONTENT OF NOTIFICATION.

(a) IN GENERAL.—Regardless of the method by which notice is provided to individuals under section 213, such notice shall include, to the extent possible—

(1) a description of the categories of sensitive personally identifiable information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person;

(2) a toll-free number—

(A) that the individual may use to contact the agency or business entity, or the agent of the agency or business entity; and

(B) from which the individual may learn what types of sensitive personally identifiable information the agency or business entity maintained about that individual; and

(3) the toll-free contact telephone numbers and addresses for the major credit reporting agencies.

(b) ADDITIONAL CONTENT.—Notwithstanding section 219, a State may require that a notice under subsection (a) shall also include information regarding victim protection assistance provided for by that State.

(c) DIRECT BUSINESS RELATIONSHIP.—Regardless of whether a business entity, agency, or a designated third party provides the notice required pursuant to section 211(b), such notice shall include the name of the business entity or agency that has a direct relationship with the individual being notified.

SEC. 215. COORDINATION OF NOTIFICATION WITH CREDIT REPORTING AGENCIES.

If an agency or business entity is required to provide notification to more than 5,000 individuals under section 211(a), the agency or business entity shall also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis (as defined in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)) of the timing and distribution of the notices. Such notice shall be given to the consumer credit reporting agencies without unreasonable delay and, if it will not delay notice to the affected individuals, prior to the distribution of notices to the affected individuals.

SEC. 216. NOTICE TO LAW ENFORCEMENT.

(a) DESIGNATION OF GOVERNMENT ENTITY TO RECEIVE NOTICE.—

(1) IN GENERAL.—Not later than 60 days after the date of enactment of this Act, the Secretary of the Department of Homeland Security shall designate a

Federal Government entity to receive the notices required under sections 212 and 216, and any other reports and information about information security incidents, threats, and vulnerabilities.

(2) RESPONSIBILITIES OF THE DESIGNATED ENTITY.—The designated entity shall—

(A) be responsible for promptly providing the information that it receives to the United States Secret Service and the Federal Bureau of Investigation, and to the Federal Trade Commission for civil law enforcement purposes; and

(B) provide the information described in subparagraph (A) as appropriate to other Federal agencies for law enforcement, national security, or data security purposes.

(b) NOTICE.—Any business entity or agency shall notify the designated entity of the fact that a security breach has occurred if—

(1) the number of individuals whose sensitive personally identifying information was, or is reasonably believed to have been accessed or acquired by an unauthorized person exceeds 5,000;

(2) the security breach involves a database, networked or integrated databases, or other data system containing the sensitive personally identifiable

information of more than 500,000 individuals nationwide;

(3) the security breach involves databases owned by the Federal Government; or

(4) the security breach involves primarily sensitive personally identifiable information of individuals known to the agency or business entity to be employees and contractors of the Federal Government involved in national security or law enforcement.

(c) FTC RULEMAKING AND REVIEW OF THRESHOLDS.—Not later 1 year after the date of the enactment of this Act, the Federal Trade Commission, in consultation with the Attorney General of the United States and the Secretary of the Department of Homeland Security, shall promulgate regulations regarding the reports required under subsection (a). The Federal Trade Commission, in consultation with the Attorney General and the Secretary of the Department of Homeland Security, after notice and the opportunity for public comment, and in a manner consistent with this section, shall promulgate regulations, as necessary, under section 553 of title 5, United States Code, to adjust the thresholds for notice to law enforcement and national security authorities under subsection (a) and to facilitate the purposes of this section.

(d) TIMING.—The notice required under subsection (a) shall be provided as promptly as possible, but such notice must be provided either 72 hours before notice is provided to an individual pursuant to section 211, or not later than 10 days after the business entity or agency discovers the security breach or discovers that the nature of the security breach requires notice to law enforcement under this section, whichever occurs first.

SEC. 217. ENFORCEMENT.

(a) IN GENERAL.—The Attorney General of the United States and the Federal Trade Commission may enforce civil violations of section 211.

(b) CIVIL ACTIONS BY THE ATTORNEY GENERAL OF THE UNITED STATES.—

(1) IN GENERAL.—The Attorney General may bring a civil action in the appropriate United States district court against any business entity that engages in conduct constituting a violation of this subtitle and, upon proof of such conduct by a preponderance of the evidence, such business entity shall be subject to a civil penalty of not more than $11,000 per day per security breach.

(2) PENALTY LIMITATION.—Notwithstanding any other provision of law, the total amount of the civil penalty assessed against a business entity for conduct

involving the same or related acts or omissions that results in a violation of this subtitle may not exceed $1,000,000.

(3) DETERMINATIONS.—The determination of whether a violation of a provision of this subtitle has occurred, and if so, the amount of the penalty to be imposed, if any, shall be made by the court sitting as the finder of fact. The determination of whether a violation of a provision of this subtitle was willful or intentional, and if so, the amount of the additional penalty to be imposed, if any, shall be made by the court sitting as the finder of fact.

(4) ADDITIONAL PENALTY LIMIT.—If a court determines under paragraph (3) that a violation of a provision of this subtitle was willful or intentional and imposes an additional penalty, the court may not impose an additional penalty in an amount that exceeds $1,000,000.

(c) INJUNCTIVE ACTIONS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—If it appears that a business entity has engaged, or is engaged, in any act or practice constituting a violation of this subtitle, the Attorney General may petition an appropriate district court of the United States for an order—

(A) enjoining such act or practice; or

(B) enforcing compliance with this subtitle.

(2) ISSUANCE OF ORDER.—A court may issue an order under paragraph (1), if the court finds that the conduct in question constitutes a violation of this subtitle.

(d) CIVIL ACTIONS BY THE FEDERAL TRADE COMMISSION.—

(1) IN GENERAL.—Compliance with the requirements imposed under this subtitle may be enforced under the Federal Trade Commission Act (15 U.S.C. 41 et seq.) by the Federal Trade Commission with respect to business entities subject to this Act. All of the functions and powers of the Federal Trade Commission under the Federal Trade Commission Act are available to the Commission to enforce compliance by any person with the requirements imposed under this title.

(2) PENALTY LIMITATION.—

(A) IN GENERAL.—Notwithstanding any other provision of law, the total sum of civil penalties assessed against a business entity for all violations of the provisions of this subtitle resulting from the same or related acts or omissions

may not exceed $1,000,000, unless such conduct is found to be willful or intentional.

(B) DETERMINATIONS.—The determination of whether a violation of a provision of this subtitle has occurred, and if so, the amount of the penalty to be imposed, if any, shall be made by the court sitting as the finder of fact. The determination of whether a violation of a provision of this subtitle was willful or intentional, and if so, the amount of the additional penalty to be imposed, if any, shall be made by the court sitting as the finder of fact.

(C) ADDITIONAL PENALTY LIMIT.—If a court determines under subparagraph (B) that a violation of a provision of this subtitle was willful or intentional and imposes an additional penalty, the court may not impose an additional penalty in an amount that exceeds $1,000,000.

(3) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—For the purpose of the exercise by the Federal Trade Commission of its functions and powers under the Federal Trade Commission Act, a violation of any requirement or prohibition imposed under this title shall constitute an unfair or deceptive act or practice in commerce in violation of a regulation under sec-

tion 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(I)(B)) regarding unfair or deceptive acts or practices and shall be subject to enforcement by the Federal Trade Commission under that Act with respect to any business entity, irrespective of whether that business entity is engaged in commerce or meets any other jurisdictional tests in the Federal Trade Commission Act.

(e) COORDINATION OF ENFORCEMENT.—

(1) IN GENERAL.—Before opening an investigation, the Federal Trade Commission shall consult with the Attorney General.

(2) LIMITATION.—The Federal Trade Commission may initiate investigations under this subsection unless the Attorney General determines that such an investigation would impede an ongoing criminal investigation or national security activity.

(3) COORDINATION AGREEMENT.—

(A) IN GENERAL.—In order to avoid conflicts and promote consistency regarding the enforcement and litigation of matters under this Act, not later than 180 days after the enactment of this Act, the Attorney General and the Commission shall enter into an agreement for coordination regarding the enforcement of this Act.

(B) REQUIREMENT.—The coordination agreement entered into under subparagraph (A) shall include provisions to ensure that parallel investigations and proceedings under this section are conducted in a matter that avoids conflicts and does not impede the ability of the Attorney General to prosecute violations of Federal criminal laws.

(4) COORDINATION WITH THE FCC.—If an enforcement action under this Act relates to customer proprietary network information, the Federal Trade Commission shall coordinate the enforcement action with the Federal Communications Commission.

(f) RULEMAKING.—The Federal Trade Commission may, in consultation with the Attorney General, issue such other regulations as it determines to be necessary to carry out this subtitle. All regulations promulgated under this Act shall be issued in accordance with section 553 of title 5, United States Code. Where regulations relate to customer proprietary network information, the promulgation of such regulations will be coordinated with the Federal Communications Commission.

(g) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this subtitle are cumulative and

shall not affect any other rights and remedies available under law.

(h) FRAUD ALERT.—Section 605A(b)(1) of the Fair Credit Reporting Act (15 U.S.C. 1681c–1(b)(1)) is amended by inserting ", or evidence that the consumer has received notice that the consumer's financial information has or may have been compromised," after "identity theft report".

SEC. 218. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) IN GENERAL.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State or any State or local law enforcement agency authorized by the State attorney general or by State statute to prosecute violations of consumer protection law, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of a business entity in a practice that is prohibited under this subtitle, the State or the State or local law enforcement agency on behalf of the residents of the agency's jurisdiction, may bring a civil action on behalf of the residents of the State or jurisdiction in a district court of the United States of appropriate jurisdiction to—

(A) enjoin that practice;

(B) enforce compliance with this subtitle; or

(C) civil penalties of not more than $11,000 per day per security breach up to a maximum of $1,000,000 per violation, unless such conduct is found to be willful or intentional.

(2) PENALTY LIMITATION.—

(A) IN GENERAL.—Notwithstanding any other provision of law, the total sum of civil penalties assessed against a business entity for all violations of the provisions of this subtitle resulting from the same or related acts or omissions may not exceed $1,000,000, unless such conduct is found to be willful or intentional.

(B) DETERMINATIONS.—The determination of whether a violation of a provision of this subtitle has occurred, and if so, the amount of the penalty to be imposed, if any, shall be made by the court sitting as the finder of fact. The determination of whether a violation of a provision of this subtitle was willful or intentional, and if so, the amount of the additional penalty to be imposed, if any, shall be made by the court sitting as the finder of fact.

(C) ADDITIONAL PENALTY LIMIT.—If a court determines under subparagraph (B) that a violation of a provision of this subtitle was will-

ful or intentional and imposes an additional penalty, the court may not impose an additional penalty in an amount that exceeds $1,000,000.

(3) NOTICE.—

(A) IN GENERAL.—Before filing an action under paragraph (1), the attorney general of the State involved shall provide to the Attorney General of the United States—

(i) written notice of the action; and

(ii) a copy of the complaint for the action.

(B) EXEMPTION.—

(i) IN GENERAL.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subtitle, if the State attorney general determines that it is not feasible to provide the notice described in such subparagraph before the filing of the action.

(ii) NOTIFICATION.—In an action described in clause (i), the attorney general of a State shall provide notice and a copy of the complaint to the Attorney General at the time the State attorney general files the action.

(b) FEDERAL PROCEEDINGS.—Upon receiving notice under subsection (a)(2), the Attorney General shall have the right to—

(1) move to stay the action, pending the final disposition of a pending Federal proceeding or action;

(2) initiate an action in the appropriate United States district court under section 217 and move to consolidate all pending actions, including State actions, in such court;

(3) intervene in an action brought under subsection (a)(2); and

(4) file petitions for appeal.

(c) PENDING PROCEEDINGS.—If the Attorney General or the Federal Trade Commission initiate a criminal proceeding or civil action for a violation of a provision of this subtitle, or any regulations thereunder, no attorney general of a State may bring an action for a violation of a provision of this subtitle against a defendant named in the Federal criminal proceeding or civil action.

(d) CONSTRUCTION.—For purposes of bringing any civil action under subsection (a), nothing in this subtitle regarding notification shall be construed to prevent an attorney general of a State from exercising the powers conferred on such attorney general by the laws of that State to—

(1) conduct investigations;

(2) administer oaths or affirmations; or

(3) compel the attendance of witnesses or the production of documentary and other evidence.

(e) VENUE; SERVICE OF PROCESS.—

(1) VENUE.—Any action brought under subsection (a) may be brought in—

(A) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or

(B) another court of competent jurisdiction.

(2) SERVICE OF PROCESS.—In an action brought under subsection (a), process may be served in any district in which the defendant—

(A) is an inhabitant; or

(B) may be found.

(f) NO PRIVATE CAUSE OF ACTION.—Nothing in this subtitle establishes a private cause of action against a business entity for violation of any provision of this subtitle.

SEC. 219. EFFECT ON FEDERAL AND STATE LAW.

For any entity, or agency that is subject to this subtitle, the provisions of this subtitle shall supersede any other provision of Federal law, or any provisions of the law of any State, relating to notification of a security breach, ex-

cept as provided in section 214(b). Nothing in this subtitle shall be construed to modify, limit, or supersede the operation of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) or its implementing regulations, including those regulations adopted or enforced by States, the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et seq.) or its implementing regulations, or the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17937) or its implementing regulations.

SEC. 220. REPORTING ON EXEMPTIONS.

(a) FTC REPORT.—Not later than 18 months after the date of enactment of this Act, and upon request by Congress thereafter, the Federal Trade Commission shall submit a report to Congress on the number and nature of the security breaches described in the notices filed by those business entities invoking the risk assessment exemption under section 212(b) and their response to such notices.

(b) LAW ENFORCEMENT REPORT.—

(1) IN GENERAL.—Not later than 18 months after the date of enactment of this Act, and upon the request by Congress thereafter, the United States Secret Service and Federal Bureau of Investigation shall submit a report to Congress on the number and nature of security breaches subject to the national secu-

rity and law enforcement exemptions under section 212(a).

(2) REQUIREMENT.—The report required under paragraph (1) shall not include the contents of any risk assessment provided to the United States Secret Service and the Federal Bureau of Investigation under this subtitle.

SEC. 221. EFFECTIVE DATE.

This subtitle shall take effect on the expiration of the date which is 90 days after the date of enactment of this Act.

TITLE III—COMPLIANCE WITH STATUTORY PAY-AS-YOU-GO ACT

SEC. 301. BUDGET COMPLIANCE.

The budgetary effects of this Act, for the purpose of complying with the Statutory Pay-As-You-Go Act of 2010, shall be determined by reference to the latest statement titled "Budgetary Effects of PAYGO Legislation" for this Act, submitted for printing in the Congressional Record by the Chairman of the Senate Budget Committee, provided that such statement has been submitted prior to the vote on passage.

Calendar No. 181

112TH CONGRESS
1ST SESSION

S. 1151

A BILL

To prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.

SEPTEMBER 22, 2011

Reported with an amendment